Waldemar NOWAKOWSKI, Zbigniew ŁUKASIK, Marcin CHRZAN

ANALIZA METOD ZAPEWNIENIA BEZPIECZEŃSTWA TRANSMISJI DANYCH W SYSTEMACH AUTOMATYKI KOLEJOWEJ

Streszczenie

Rozwój systemów automatyki kolejowej jest procesem badawczym, w którym dąży się m.in. do stosowania nowoczesnych technologii [1, 15, 16]. Jednym z aktualnych obszarów badawczych jest zapewnienie bezpieczeństwa bezprzewodowej transmisji danych w rozproszonych systemach automatyki kolejowej [5, 6, 7, 8]. W artykule przedstawiono analizę metody zapewnienia bezpieczeństwa transmisji danych w rozproszonych systemach wykorzystujących transmisję bezprzewodową. Szczególną uwagę poświęcono ocenie wybranych metod kryptograficznych.

WSTĘP

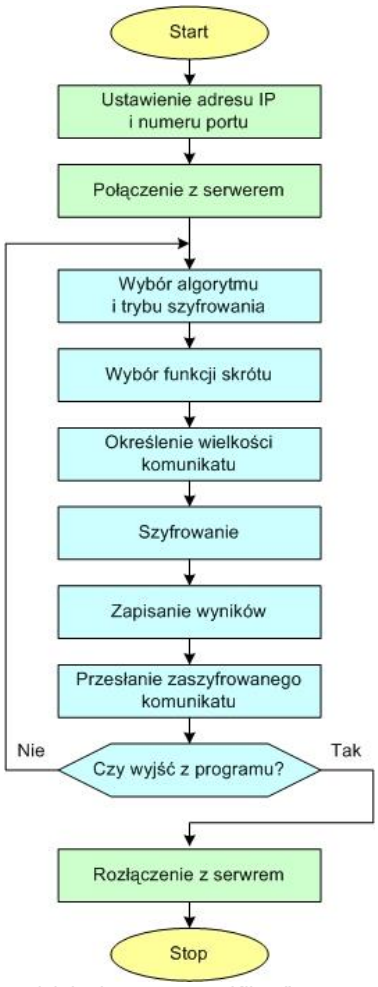
Komputerowe systemy sterowania automatyki kolejowej można traktować jako rozproszone systemy czasu rzeczywistego (*Distributed Real Time Systems*) [2, 4, 10, 13]. W większości przypadków mamy bowiem do czynienia z rozproszeniem przetwarzania danych, które musi uwzględniać ograniczenia czasowe (*timing constraints*). Ponieważ wymiana informacji w takich systemach odbywa się za pośrednictwem sieci komputerowej, istotnym jest zachowanie determinizmu czasowego przy przesyłaniu telegramów. Za czynniki krytyczne, w stosowaniu funkcji bezpieczeństwa należy uznać przekroczenie maksymalnego czasu realizacji algorytmu kryptograficznego lub tworzenie zbyt dużych bloków danych. Może to bowiem skutkować brakiem możliwości przesłania danych przy zadanej przepustowości kanału transmisyjnego (*bandwidth*) w określonym czasie [3, 5]. Niezbędne jest więc przeprowadzenie analizy opóźnień powstałych w wyniku realizacji funkcji bezpieczeństwa tj.: przygotowania danych do transferu oraz późniejszego ich rozkodowania.

1. OPROGRAMOWANIE BADAWCZE

W celu weryfikacji metod przeciwdziałania zagrożeniom, które mogą być zastosowane w procesie bezprzewodowej wymiany danych przez systemy automatyki kolejowej opracowano specjalizowane oprogramowanie badawcze. W oprogramowaniu tym, które składa się z dwóch modułów (Klient, Serwer) uwzględniono wybrane metody obrony przez zagrożeniami, w tym szyfry blokowe: Blowfish, Twofish, DES, 3DES, AES-128, AES-192 i AES-256 dla trybów: ECB, CBC, PCBC, CFB, OFB i CTR oraz kody integralności: MD-5, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 i SHA-512/256 [12, 14]. Oprogramowanie umożliwia tworzenie telegramów typu B0, tj. z zaszyfrowaną wiadomością i kodem integralności danych [11].

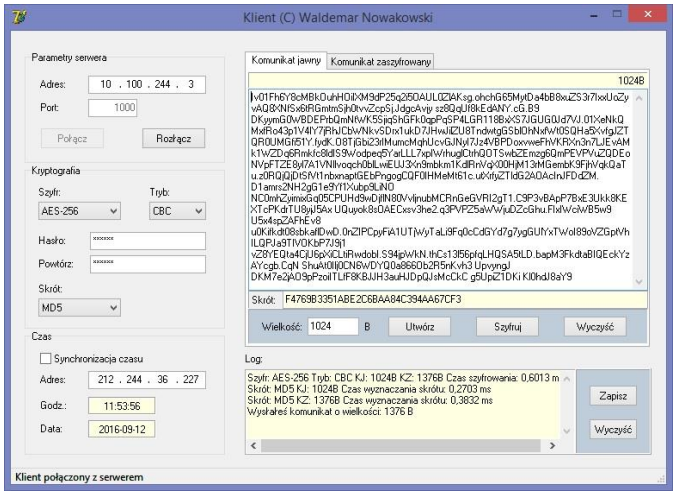
1.1. Program – Klient

Program „Klient" jest odpowiedzialny za generowanie, szyfrowanie i przesyłanie komunikatów do modułu „Serwer". Użytkownik ma możliwość wyboru algorytmu i trybu szyfrowania oraz metody wyznaczania kodu integralności danych. Wielkość generowanego komunikatu jest definiowana przez użytkownika. Komunikacja pomiędzy modułem „Klient" i „Serwer" wykorzystuje protokół TCP/IP. Dlatego też, w celu nawiązania połączenia z modułem „Serwer" użytkownik musi podać adres IP serwera i numer aktywnego portu. Główną funkcjonalnością programu „Klient", oprócz wcześniej wymienionych, jest pomiar czasu szyfrowania i generowania kodu integralności danych. Pozwala to na badanie wpływu wielkości komunikatu na opóźnienia wnoszone w procesie szyfrowania i wyznaczania kodów integralności danych. Algorytm programu „Klient" został przedstawiony na rysunku 1.



Rys. 1. *Algorytm działania programu „Klient"*

Przykładowy ekran główny programu „Klient" przedstawiono na rysunku 2.

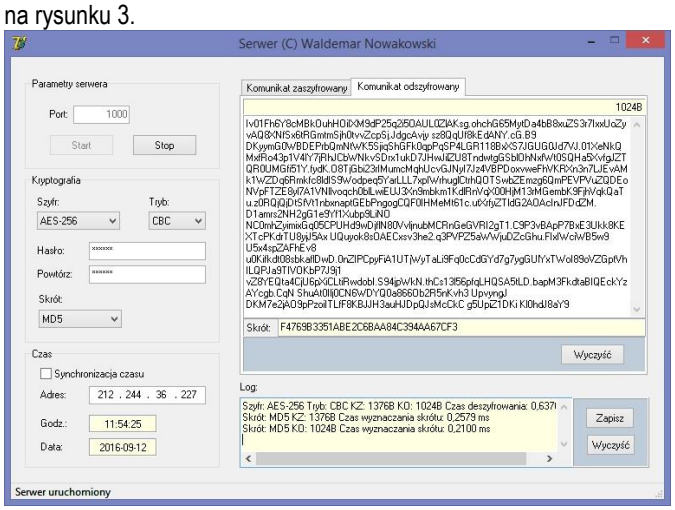


Rys. 2. *Ekran główny programu „Klient”*

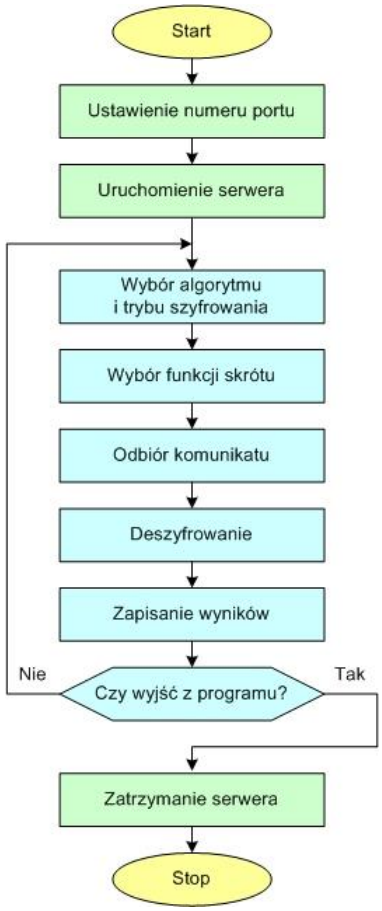
1.2. Program – Serwer

Program „Serwer” jest odpowiedzialny za odbiór i deszyfrowanie komunikatów wysyłanych przez moduł „Klient”. Użytkownik ma możliwość wyboru algorytmu i trybu szyfrowania oraz metody wyznaczania kodu integralności danych. Parametry te, przy badaniu kolejnych komunikatów, powinny być ustawione identycznie jak w programie „Klient”. Nie przewidziano bowiem automatycznego rozpoznawania w/w parametrów przez moduł „Serwer”, na przykład poprzez uwzględnienie tych danych w przesyłanych telegramach. Komunikacja pomiędzy modułem „Serwer” i „Klient” jest realizowana przy wykorzystaniu protokołu TCP/IP. Dlatego też, w celu umożliwienia nawiązania połączenia przez moduł „Klient”, użytkownik musi podać numer portu i uruchomić serwer. Kolejną funkcjonalnością programu „Serwer” jest pomiar czasu deszyfrowania i generowania kodu integralności danych. Pozwala to na ocenę wpływu wielkości komunikatu na opóźnienia wnoszone w procesie deszyfrowania i wyznaczania kodów integralności danych. Algorytm programu „Serwer” został przedstawiony na rysunku 4.

Przykładowy ekran główny programu „Serwer” przedstawiono na rysunku 3.



Rys. 3. *Ekran główny programu „Serwer”*



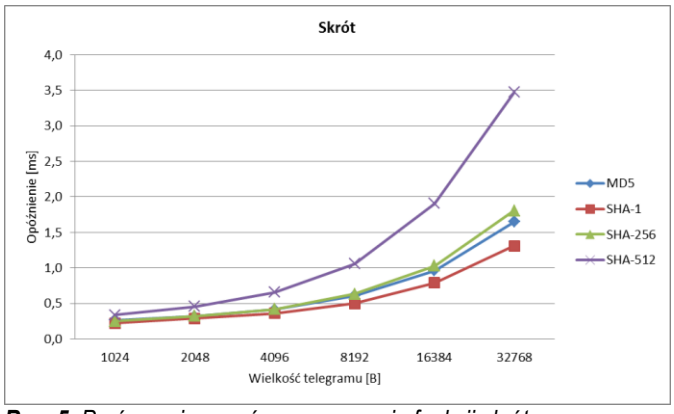
Rys. 4. *Algorytm działania programu „Serwer”*

2. ANALIZA ALGORYTMÓW WYZNACZANIA FUNKCJI SKRÓTU

Badanie przeprowadzono dla wybranych funkcji skrótu tj.: MD-5, SHA-1, SHA-256, SHA-512, przy uwzględnieniu różnych wielkości bloków danych: 1024, 2048, 4096, 8192, 16384, 32768 [B]. Wyniki badania opóźnienia wnoszonego przez funkcje skrótu przedstawiono w tabeli 1 i w formie graficznej na rysunku 5.

Tab. 1. *Zestawienie czasów wyznaczania funkcji skrótu*

	1024 [B]	**2048** [B]	**4096** [B]	**8192** [B]	**16384** [B]	**32768** [B]
MD5	0,27 ms	0,32 ms	0,41 ms	0,61 ms	0,96 ms	1,65 ms
SHA-1	0,22 ms	0,29 ms	0,36 ms	0,50 ms	0,79 ms	1,31 ms
SHA-256	0,25 ms	0,32 ms	0,42 ms	0,63 ms	1,03 ms	1,81 ms
SHA-512	0,34 ms	0,46 ms	0,66 ms	1,06 ms	1,91 ms	3,47 ms



Rys. 5. *Porównanie czasów wyznaczania funkcji skrótu*

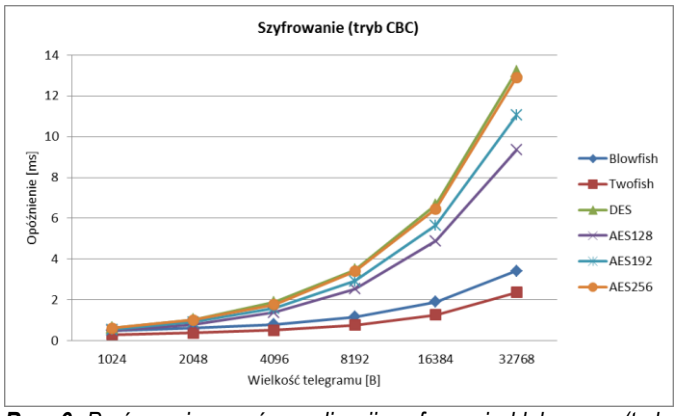
Największe opóźnienia występują dla algorytmu SHA-512. Pozostałe metody generują podobne czasy realizacji funkcji skrótu.

3. ANALIZA ALGORYTMÓW SZYFROWANIA DANYCH

Analizie poddane zostały następujące algorytmy szyfrowania blokowego: Blowfish, Twofish, DES, AES128, AES192, AES256 przy uwzględnieniu różnych trybów szyfrowania: ECB, CBC, CFB, OFB i CTR. Z przeprowadzonych badań wynika, że wybór trybu szyfrowania nie wpływa na wielkość opóźnienia, a tym samym należy stosować bardziej bezpieczne tryby tj.: CBC (*cipher-block chaining*) lub CFB (*cipher feedback*) w miejsce trybu ECB (*electronic codebook*). W przypadku algorytmów szyfrowania blokowego, najmniejsze czasy realizacji funkcji bezpieczeństwa występują dla algorytmów: Blowfish, Twofish, które wykorzystują klucze 128-bitowe. Najdłuższy czas szyfrowania i deszyfrowania występuje dla algorytmów AES-256 i DES. Ze względu na poziom bezpieczeństwa należy jednak stosować algorytm AES zabezpieczany kluczem 256-bitowym zamiast algorytmu DES, który ma klucz 56-bitowy. Wyniki badań opóźnienia wnoszonego przez różne algorytmy (tryb CBC) odpowiednio dla szyfrowania i deszyfrowania przedstawiono w tabeli 2 i 3 oraz w formie graficznej na rysunku 6 i 7.

Tab. 2. *Zestawienie czasów szyfrowania blokowego (tryb CBC)*

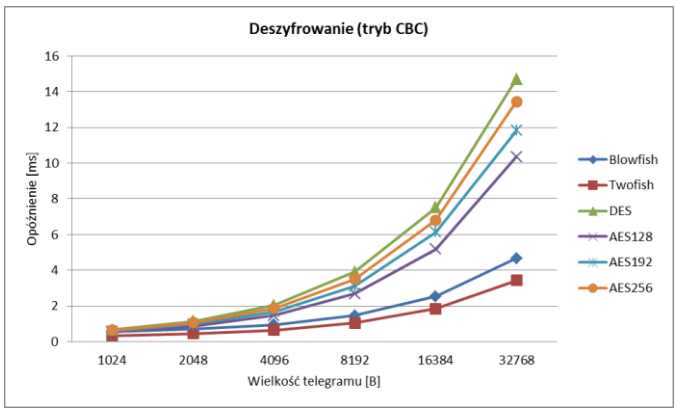
	1024 [B]	**2048** [B]	**4096** [B]	**8192** [B]	**16384** [B]	**32768** [B]
Blowfish	0,49 [ms]	0,61 [ms]	0,79 [ms]	1,17 [ms]	1,89 [ms]	3,41 [ms]
Twofish	0,29 [ms]	0,38 [ms]	0,51 [ms]	0,77 [ms]	1,27 [ms]	2,36 [ms]
DES	0,63 [ms]	1,04 [ms]	1,88 [ms]	3,46 [ms]	6,66 [ms]	13,21 [ms]
AES128	0,49 [ms]	0,79 [ms]	1,37 [ms]	2,53 [ms]	4,89 [ms]	9,35 [ms]
AES192	0,5482 [ms]	0,9146 [ms]	1,5847 [ms]	2,9242 [ms]	5,66 [ms]	11,05 [ms]
AES256	0,6131 [ms]	1,0071 [ms]	1,7701 [ms]	3,3957 [ms]	6,46 [ms]	12,91 [ms]



Rys. 6. *Porównanie czasów realizacji szyfrowania blokowego (tryb CBC)*

Tab. 2. *Zestawienie czasów deszyfrowania blokowego (tryb CBC)*

	1024 [B]	**2048** [B]	**4096** [B]	**8192** [B]	**16384** [B]	**32768** [B]
Blowfish	0,54 [ms]	0,72 [ms]	0,95 [ms]	1,47 [ms]	2,53 [ms]	4,68 [ms]
Twofish	0,33 [ms]	0,45 [ms]	0,64 [ms]	1,05 [ms]	1,84 [ms]	3,43 [ms]
DES	0,67 [ms]	1,14 [ms]	2,03 [ms]	3,91 [ms]	7,52 [ms]	14,71 [ms]
AES128	0,54 [ms]	0,85 [ms]	1,46 [ms]	2,68 [ms]	5,18 [ms]	10,36 [ms]
AES192	0,59 [ms]	0,96 [ms]	1,66 [ms]	3,10 [ms]	6,14 [ms]	11,82 [ms]
AES256	0,64 [ms]	1,06 [ms]	1,87 [ms]	3,50 [ms]	6,80 [ms]	13,44 [ms]



Rys. 7. *Porównanie czasów realizacji deszyfrowania blokowego (tryb CBC)*

PODSUMOWANIE

Rozwój technologii sieciowych spowodował, że współczesne komputerowe systemy automatyki kolejowej są w dużej mierze rozproszonymi systemami czasu rzeczywistego. Należy, więc przy ich projektowaniu uwzględniać czas reakcji na zmiany zachodzące w sterowanych obiektach, który jest wypadkową czasów reakcji pojedynczych urządzeń sterowania ruchem. Mówimy wówczas, że system zachowuje determinizm czasowy, czyli uwzględnia czasy reakcji pojedynczych elementów systemu rozproszonego. Istotnym staje się w takich przypadkach wybór metod, które zapewnią wymaganą szybkość wymiany danych przy zachowaniu ich integralności oraz poufności. Przeprowadzone badania eksperymentalne umożliwiły oszacowanie czasu potrzebnego na wyznaczanie kodów integralności i szyfrowanie danych, przy uwzględnieniu różnych algorytmów kryptograficznych. Uzyskane wyniki badań mogą być bardzo pomocne przy opracowywaniu nowych systemów automatyki kolejowej, w których planuje się zastosowanie bezprzewodowej transmisji danych.

BIBLIOGRAFIA

1. Ai B., Cheng X., Kuerner T. et al. *Challenges Toward Wireless Communications for High-Speed Railway*, IEEE Transactions on Intelligent Transportation Systems, Volume: 15, Issue: 5, Pages: 2143-2158, 2014
2. Aguado M., Jacob E., Saiz P. et al. *Railway signaling systems and new trends in wireless data communication*, 62nd IEEE Vehicular Technology Conference, Dallas, USA, IEEE VTS Vehicular Technology Conference Proceedings, Pages: 1333-1336, 2005.
3. Briso C., Alonso J.I., *Requirements of wireless communications for control and operation of railway systems*, 46th Annual Congress of the Federation-of-Telecommunications-Engineers-of-the-European-Union (FITCE), Warsaw, Poland, 2007, Journal of the Institute of Telecommunications Professionals, Volume: 1, Pages: 13-18, Part: 1
4. Liem M., Mendiratta V.B., *Mission critical communication networks for railways*, Bell Labs Technical Journal, Volume: 16, Issue: 3, Pages: 29-46, 2011.
5. Łukasik Z., Nowakowski W., *Bezprzewodowe systemy sterowania ruchem kolejowym*, Infrastruktura Transportu, nr 4/2013, str. 22-25,2013.
6. Łukasik Z., Nowakowski W., *Wymiana informacji w systemach związanych z bezpieczeństwem*, Logistyka 6/2008, 2008.
7. Łukasik Z., Nowakowski W., Kuśmińska-Fijałkowska A., *Zarządzanie bezpieczeństwem infrastruktury krytycznej*, Logistyka 4/2014, str. 758-763, 2014.

8. Nowakowski W., *Information security and privacy protection in emergency management software systems*, Logistyka 4/2015, str. 8072-8077, 2015.
9. Nowakowski W., Warchoł A., *Nowoczesne systemy sterowania i diagnostyki na przykładzie LCS Drzewica*, Zeszyty Naukowo-Techniczne Stowarzyszenia Inżynierów i Techników Komunikacji w Krakowie, Seria: Materiały Konferencyjne, Wydanie 95 z. 154, str. 453-465, 2010.
10. Nowakowski W., Szczygielski M., *Analiza bezpieczeństwa transmisji w systemie zabezpieczenia przejazdów SZP-1*, XVI Międzynarodowa Konferencja „TransComp", Zakopane 2012r.
11. PN-EN 50159:2011, *Zastosowania kolejowe - Systemy łączności, sterowania ruchem i przetwarzania danych - Łączność bezpieczna w systemach transmisyjnych*, PKN, 2011.
12. Schneier B., *Kryptografia dla praktyków. Protokoły, algorytmy i programy źródłowe z języku C*, PWN, Warszawa, 2002.
13. Song Y. Kim J., Choi S.W. et al., *Long Term Evolution for Wireless Railway Communications: Testbed Deployment and Performance Evaluation*, IEEE Communications Magazine, Volume: 54, Issue: 2, Pages: 138-145, 2016.
14. Stallings W.., *Kryptografia i bezpieczeństwo sieci komputerowych. Matematyka szyfrów i techniki kryptologii*, Helion, Gliwice, 2011.
15. Wu D., Zhang N., *Research of Wireless Transmission Strategy for High-Speed Railway*, International Conference on Computer Science and Information Technology (CSAIT), Kunming, China, 2013, Proceedings of International Conference on Computer Science and Information Technology, Part III, Pages 221-230.
16. Yan L., Fang X., Fang Y., *Control and Data Signaling Decoupled Architecture for Railway Wireless Networks*, IEEE Wireless Communications, Volume: 22, Issue: 1, Pages: 103-111, 2015

ANALYSIS OF METHODS TO ENSURE THE SECURITY OF DATA TRANSMISSION IN THE RAILWAY TRAFFIC CONTROL SYSTEMS

Abstract

Development of railway traffic control systems is the research process, which aim is, among others, to implement the modern technologies in such systems. One of the current research areas is to provide the security of wireless data transmission in distributed railway traffic control systems. In the article an analysis of the current methods which ensure the security of wireless data transmission in distributed systems were presented. Particular attention was given to the assessment of selected cryptographic methods

Autorzy:
dr inż. **Waldemar Nowakowski** – Uniwersytet Technologiczno-Humanistyczny im. Kazimierza Pułaskiego w Radomiu, Wydział Transportu i Elektrotechniki, 26-600 Radom, ul. Malczewskiego 29, e-mail: w.nowakowski@uthrad.pl
prof. dr hab. inż. **Zbigniew Łukasik** – Uniwersytet Technologiczno-Humanistyczny im. Kazimierza Pułaskiego w Radomiu, Wydział Transportu i Elektrotechniki, 26-600 Radom, ul. Malczewskiego 29, e-mail: z.lukasik@uthrad.pl
dr hab. inż. **Marcin Chrzan** – Uniwersytet Technologiczno-Humanistyczny im. Kazimierza Pułaskiego w Radomiu, Wydział Transportu i Elektrotechniki, 26-600 Radom, ul. Malczewskiego 29, e-mail: m.chrzan@uthrad.pl