Marcin CHRZAN, Paweł PIROSZ

METODA SZYFROWANIA TELEGRAMÓW KOLEJOWYCH TRANSMITOWANYCH W SIECIACH OTWARTYCH Z WYKORZYSTANIEM TECHNOLOGII LTE

Streszczenie

W artykule przedstawiono rozważania na temat wykorzystania na kolei zabezpieczeń otwartych systemów radiowych zgodnie z normą normie PN-EN 50159:2010. Zaprezentowano ogólne wyniki badań w zakresie metod szyfrowania i wpływu ich na opóźnienia w transmisji sygnału radiowego.

WSTĘP

W artykule tym zostanie przedstawione autorskie podejście do normy PN EN 50159:2010 pozwalające na wykorzystanie radiowych sieci otwartych systemu LTE w radiołączności kolejowej. Systemy radiowe otwarte są obecnie szeroko rozważane, jako medium transmisji danych pomiędzy poszczególnymi elementami infrastruktury kolejowej. Ze względu na specyficzny charakter zarówno transmisji jak i dostępu do niej osób postronnych, muszą te systemy spełniać wysokie normy bezpieczeństwa. Dla systemów kolejowych to zagadnienie reguluje szczegółowo norma PN EN 50159:2010 [3]. Dlatego też istnieje potrzeba spełnienia wymogów bezpieczeństwa, jakie określa w/w norma w celu osiągnięcia przez cały system wykorzystujący systemy łączności bezprzewodowej otwartej zakładanego poziomu nienaruszalności bezpieczeństwa SIL (Safety Integrity Level) [1, 2, 3].

W dalszej części tego artykułu zostaną przedstawione potencjalne zagrożenia ze strony „osób trzecich" i metody przeciwdziałania tym zagrożeniom w celu zapewnienia takiej transmisji odpowiedniego poziomu bezpieczeństwa. Zostaną także przedstawione kryteria, jakie należy uwzględniać przy projektowaniu systemów otwartych dla potrzeb sterowania ruchem kolejowym, które zostaną wykorzystane do symulacji transmisji danych w standardzie LTE w oparciu o normę PN EN 50159:2010 pomiędzy urządzeniami będącymi w ruchu.

1. ZAGROŻENIA BEZPIECZEŃSTWA TRANSMISJI DANYCH W OTWARTYCH SYSTEMACH RADIOWYCH KOLEJOWYCH SYSTEMÓW STEROWANIA RUCHEM

Ze względu na otwarty układ transmisyjny bezpieczeństwo wymiany informacji w każdym systemie o ograniczonym dostępie należy oprzeć na następujących działaniach [4]:

- podejściu do systemu transmisji, jako systemu nie godnego pełnego zaufania, niezależnie od tego jakie stosuje on wewnętrzne zabezpieczenia;
- bezpiecznych funkcjach transmisyjnych;
- bezpiecznych funkcjach dostępu.

Głównym zagrożeniem dla systemu, wynikającym z niezaufanego systemu transmisyjnego, jest niepowodzenie w uzyskaniu przez odbiorcę ważnego i autentycznego telegramu. Stan taki może być spowodowany przez:

- powtórzenie telegramu (repetition);
- skasowanie telegramu (deletion);
- utworzenie telegramu przez nieautoryzowanego nadawcę (insertion);
- zmianę kolejności telegramów (resequence);
- uszkodzenie telegramu (corruption);
- opóźnienie w odebraniu telegramu (delay);
- maskaradę (masquerade).

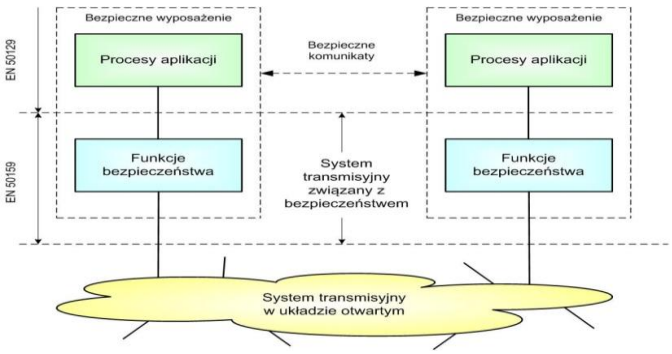
Zagrożenia te są wynikiem m.in. nieznanej liczby użytkowników, którzy mogą chcieć uzyskać dostęp do sieci oraz nieznanej liczby oraz rodzaju sprzętu, który może zostać włączony do sieci. Stwarza to potencjalne zagrożenie dla bezpieczeństwa systemu, głównie z faktu możliwości pojawienia się danych o nieznanych formatach, jak również nieznanych ilościach, a także możliwości wystąpienia ataków sieciowych ze strony nieautoryzowanych użytkowników.

2. FUNKCJE BEZPIECZEŃSTWA TRANSMISJI DANYCH W OTWARTYCH SYSTEMACH RADIOWYCH KOLEJOWYCH SYSTEMÓW STEROWANIA RUCHEM

Struktura systemu związanego z bezpieczeństwem podłączonego do otwartego układu transmisji przedstawiono na rysunku 1.

Wykorzystywany w każdym środowisku system transmisji radiowej, z punktu widzenia bezpieczeństwa należy traktować, jako niezaufany. W celu ograniczenia zagrożeń ze strony otwartego układu transmisyjnego można wziąć pod uwagę następujące warunki:

- autentyczność telegramów;
- integralność telegramów;
- czas przesyłania telegramów;
- ustalona sekwencja telegramów.



Rys.1. *Struktura systemu związanego z bezpieczeństwem podłączonego do otwartego układu transmisji [3]*

Przyjmując jako podstawę w/w warunki norma PN EN 50159:2010 podaje szereg metod zapewnienia bezpieczeństwa danych w systemach z otwartym układem transmisji, które określono jako funkcje bezpieczeństwa [3]:
- numerowanie telegramów (sequencenumber);
- stosowanie w telegramach znaczników czasu (timestamp);
- zdefiniowanie maksymalnego czasu oczekiwania na odpowiedź (time-out);
- dodawanie do telegramów identyfikatora nadawcy i odbiorcy;
- stosowanie komunikatów zwrotnych (freedbackmessage);
- wykorzystywanie procedur autoryzacji (identification);
- stosowanie kodów bezpieczeństwa (safetycode);
- szyfrowanie danych (cryptographics).

2.1. Numerowanie telegramów

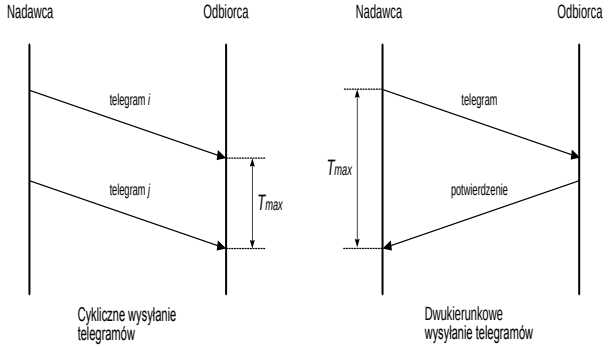
Do treści telegramów, wymienianych pomiędzy nadawcą i odbiorcą, można dopisywać kolejne numery (tzw. numery sekwencyjne), umożliwiając tym samym odbiorcy zweryfikowanie poprawności otrzymanego telegramu. Biorąc pod uwagę w/w metodę, jako sposób zwiększenia wiarygodności otrzymywanych wiadomości, należy zadbać o inicjalizację procesu numerowania telegramów i kontrolę maksymalnej wielkości licznika telegramów oraz jednolity czas w systemie.

2.2. Stosowanie w telegramach znaczników czasu

Jednym z rozwiązań, które można traktować, jako formę kontroli poprawności przesyłanych w sieci danych jest uwzględnienie związków czasowych w procesie wysyłania i odbierania telegramów. Podobnie jak w przypadku numerów sekwencyjnych, telegramy mogą być oznaczane przez stemple czasu. Pozwala to odbiorcy zweryfikować poprawności procesu wymiany informacji, na przykład poprzez kontrolę upływu czasu. Takie rozwiązanie jest jednak możliwe tylko przy zapewnieniu synchronizacji czasu w sieci informatycznej poprzez wykorzystanie systemu jednolitego czasu.

Zdefiniowanie maksymalnego czasu oczekiwania na odpowiedź

W przypadku systemu transmisyjnego pracującego w układzie otwartym i związanego z tym zmiennego ruchu sieciowego, może dochodzić do niepowodzenia w uzyskiwaniu przez odbiorcę telegramów w odpowiednim czasie. Z punktu widzenia użytkownika systemu bardzo duże znaczenie ma, jakość oferowanych usług sieciowych i wynikająca stąd potrzeba monitorowania pracy sieci. Spodziewając się wystąpienia opóźnień w dostarczaniu telegramów można zdefiniować czas time-out (Tmax), czyli maksymalny odstęp czasu między kolejnymi telegramami lub między wysłaniem telegramu i otrzymaniem potwierdzenia (rys. 2).



Rys. 2. *Graficzna interpretacja czasu time-out [3]*

2.3. Dodawanie do telegramów identyfikatora nadawcy i odbiorcy

Kolejną metodą pozwalającą na weryfikację przesyłanych w sieci danych jest stosowanie identyfikatora nadawcy i odbiorcy. W metodzie tej telegramy powinny zawierać identyfikator źródła lub przeznaczenia albo zarówno jeden jak i drugi. Taka dodatkowo przesyłana informacja umożliwia sprawdzenie, czy telegramy pochodzą od oczekiwanego nadawcy, a także pozwala na kontrolę przez odbiorcę, czy odebrane telegramy są przeznaczone dla niego. Umieszczenie tej metody na liście funkcji bezpieczeństwa wymaga jednak zapewnienia unikalności identyfikatorów.

2.4. Stosowanie komunikatów zwrotnych

Jeśli istnieje taka możliwość należy wysyłać do nadawcy komunikat zwrotny (potwierdzenie), zamieszczając w nim np. [5]:
- dane pobrane z telegramu nadawcy, w identycznej bądź zmienionej formie;
- dane będące informacjami o odbiorcy potwierdzenia;
- dane istotne z punktu widzenia bezpieczeństwa.

Zastosowanie komunikatów zwrotnych upewnia nadawcę o dostarczeniu i poprawnym odczytaniu (bądź nie) telegramu przez odbiorcę.

2.5. Wykorzystywanie procedur autoryzacji

W systemach związanych z bezpieczeństwem, otwarte układy transmisji wprowadzają zagrożenie polegające na umożliwieniu otrzymania przez system telegramów od nieznanych użytkowników, które mogą być błędnie uznane za poprawne i pochodzące z wiarygodnego źródła. W celu eliminacji tego zagrożenia zaleca się stosowanie procedury autoryzacji. Autoryzacja (authorization) polega na sprawdzaniu czy obiekt (użytkownik, aplikacja), który żąda dostępu do określonego zasobu systemu jest do tego upoważniony. Ta funkcja realizowana jest zwykle przez system operacyjny lub dedykowane oprogramowanie (firewall).

2.6. Wybór metod obrony przed zagrożeniami konstrukcji bezpiecznych telegramu w otwartej transmisji radiowej systemów sterowania ruchem kolejowym

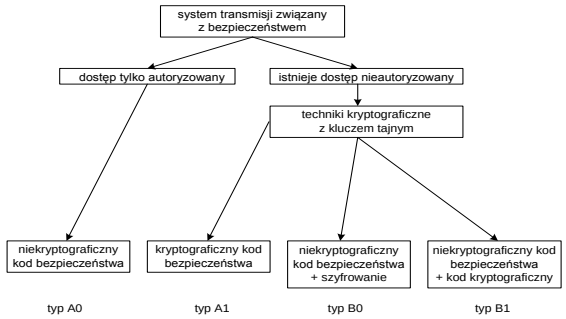
Na podstawie normy PN-EN 50159:2010 w tabeli 1 podano zestawienie zagrożeń i metod obrony przed zagrożeniami (funkcji bezpieczeństwa).

Tab. 1 *Zestawienie zagrożeń i metod obrony [3]*

	A	B	C	D	E	F	G	H
Powtórzenie (repetition)	X	X						
Skasowanie (deletion)	X							
Brak autoryzacji (insertion)	X			X	X	X		
Zmiana kolejności (resequence)	X	X						
Uszkodzenie (corruption)							X	X
Opóźnienie (delay)		X	X					
Maskarada (masquerade)					X	X		X

A. numerowanie telegramów (sequencenumber);
B. stosowanie w telegramach znaczników czasu (timestamp);
C. zdefiniowanie maksymalnego czasu oczekiwania na odpowiedź (time-out);
D. dodawanie do telegramów identyfikatora nadawcy i odbiorcy;
E. stosowanie komunikatów zwrotnych (freedbackmessage);
F. wykorzystywanie procedur autoryzacji (identification);
G. stosowanie kodów bezpieczeństwa (safetycode);
H. szyfrowanie danych (cryptographics).

Jeśli w całym cyklu życia systemu wykluczymy nieautoryzowany dostęp wówczas nie musimy stosować technik kryptograficznych, a wyłącznie kody integralności danych, które zabezpieczą transmisję przed przypadkowymi błędami. Telegramy zabezpieczone w ten sposób oznaczane są w normie PN-EN 50159:2010 jako typ A0 (rys. 3). Najczęściej takie rozwiązanie stosuje się w przypadku sieci lokalnych (LAN).



Rys. 3. *Metody zabezpieczenia transmisji dla systemów związanych z bezpieczeństwem [3]*

Natomiast jeśli przewidywany jest dostęp nieuprawniony telegramy należy zabezpieczać wg. Typu A1, B0 czy B1. Dlatego też w dalszej części artykułu zostanie przedstawiona metoda oparta o typ B0. Norma PN-EN 50159:2010, podaje również zalecenia w zakresie doboru algorytmów wyznaczania kodów bezpieczeństwa w zależności od typów telegramów, które przedstawiono w tabeli 2.

Tab. 2. *Zestawienie kodów bezpieczeństwa dla różnych typów telegramów [3]*

Typ	Rodzaj modelu telegramu dla systemu bezpieczeństwa transmisji			
	A0	A1	B0	B1
CRC	R	US	-	R
MAC	R	HR	R	R
Hashcode	R	US	HR	HR
Digital signature	R	R	R	R

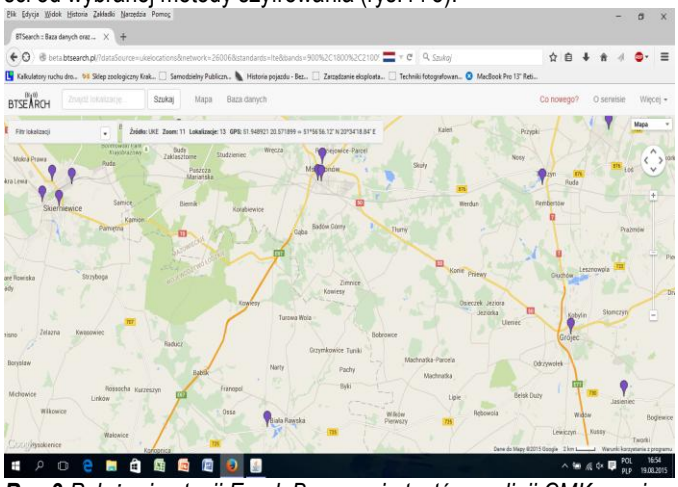
Oznaczenia:
„HR" - oznacza, że ten typ kodu bezpieczeństwa jest bardzo polecany;
„R" - oznacza, że ten typ kodu bezpieczeństwa jest polecany;
„-" - oznacza, że ten typ kodu bezpieczeństwa nie ma żadnych rekomendacji,
za czy przeciw użyciu;
„US" - oznacza, że ten typ kodu bezpieczeństwa nie jest zalecany.

W zakresie algorytmów szyfrowania w normie PN-EN 50159:2010 zaleca się stosowanie sprawdzonych algorytmów szyfrowania takich jak DES. Oficjalnym następcą DES jest algorytm AES. Poziom bezpieczeństwa dla AES wyższy ze względu na dłuższy niż w DES klucz szyfrujący. W zakresie doboru algorytmów szyfrowania norma PN-EN 50159:2010, nie zaleca stosowania trybu szyfrowania blokowego ECB w przypadku, gdy wielkości bloków danych wejściowych (przed zaszyfrowaniem) są większe niż po szyfrowaniu.

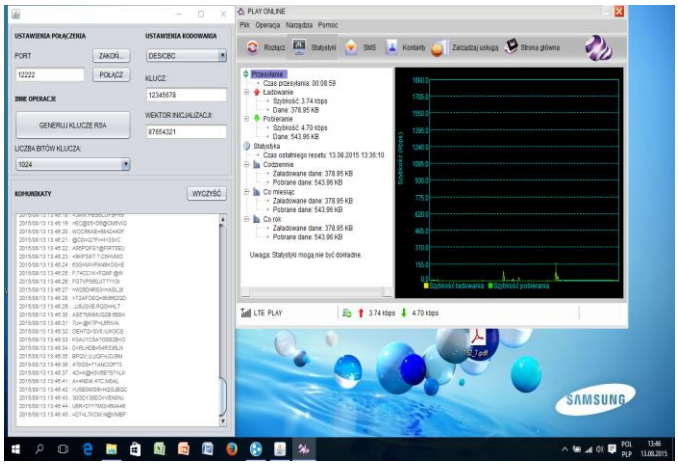
Z przedstawionej powyżej analizy wynika, że przy zastosowaniu odpowiednich technik zabezpieczenia transmisji można ją prowadzić w kanale otwartym przy stresowaniu urządzeniami kolejowymi. Właściwości te będą zaimplementowane i szerzej omówione w rozdziale piątym rozprawy wraz z ogólnym dowodem bezpieczeństwa takiego systemu.

3. METODA BADAWCZA

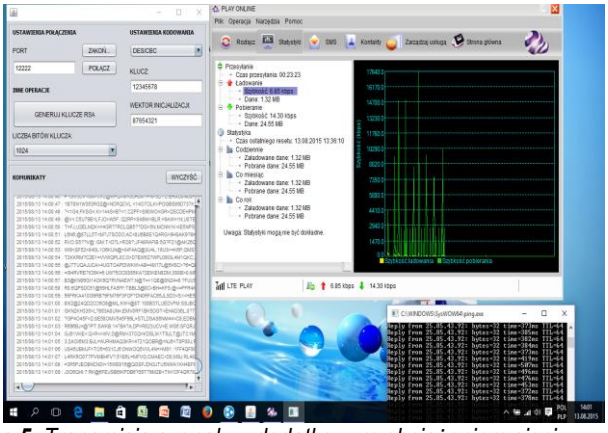
Do badań późnień w transmisji danych telegramów kolejowych wykorzystano specjalnie do tego celu oprogramowanie, w którym zaaplikowano metody szyfrowania zgodne z normą PN-EN 50159:2010. Na rysunkach poniżej przedstawiono trasę na której badania były prowadzone (rys.3) oraz pomiary opóźnień w zależności od wybranej metody szyfrowania (rys.4 i 5).



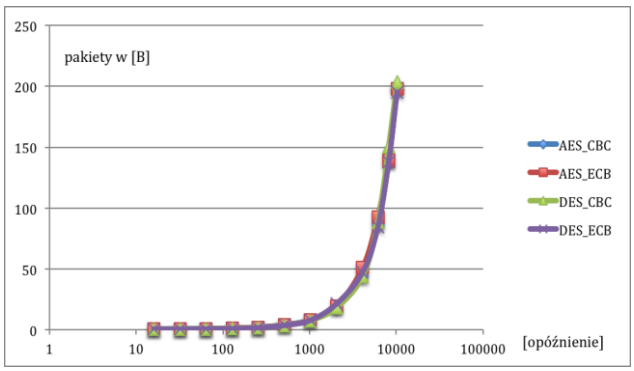
Rys.3 *Położenie stacji EnodeB w czasie testów na linii CMK pomiędzy Mszczonowem a Biała Rawską[źródło:www.btsserch.pl]*



Rys.4 *Transmisja sygnału bez dodatkowego obciążenia sieci*



Rys.5. *Transmisja sygnału z dodatkowym obciążeniem sieci*



***Rys. 6** Wpływ metody szyfrowania na opóźnienie transmisji*

Na podstawie przedstawionych wyników można stwierdzić, że rodzaj szyfrowania nie wpływa na opóźnienie pakietów, jak również długość szyfrowanych danych przy różnych technikach szyfrowania nie wpływa na opóźnienie. Dlatego też wydaję się, że przy przesyłaniu komunikatów z wykorzystaniem technologii LTE możemy wykorzystać dowolną strukturę szyfrogramu zalecaną przez normę PN-EN 50159:2010.

PODSUMOWANIE

W wyniku przedstawionych rozważań, można stwierdzić, że z powodzeniem można wykorzystać sieci otwarte do transmisji sygnałów radiowych kolejowych telegramów systemów srk. A wskazane w normie PN-EN 50159:2010 metody zabezpieczeń wpływają jedynie na bezpieczeństwo a nie mają wpływu na opóźnienia sygnału. Co więcej trzeba zaznaczyć, że sama sieć wykorzystuje metody szyfrowania, które stanowią naturalne zabezpieczenie transmisji.

BIBLIOGRAFIA

1. PN-EN 50128:2002 - Zastosowania kolejowe. Łączność, sygnalizacja i systemy sterowania. Programy dla kolejowych systemów sterowania i zabezpieczania, PKN 2007r.
2. PN-EN 50129:2007 - Zastosowania kolejowe. Systemy łączności, przetwarzania danych i sterowania ruchem –Elektroniczne systemy sterowania ruchem związane z bezpieczeństwem, PKN 2007r.
3. PN-EN 50159:2010 - Zastosowania kolejowe. Łączność, sygnalizacja i systemy sterowania., PKN 2010r.
4. Jaźwiński J., Ważyńska – Fiok K.: „Bezpieczeństwo i niezawodność systemu sterowania ruchem kolejowym”, Zeszyt 95, WKiŁ Warszawa 1982

THE ENCRYPTION METHOD OF RAILWAY TELEGRAMS TRANSMITTED ON OPEN NETWORKS USING ON LTE TECHNOLOGY

Abstract

Paper presents considerations on the use of open security on the railway radio systems in accordance with standard PN-EN 50159 : 2010 . General presented the results of research on encryption methods and the impact of delays in transmission of radio signal.

Autorzy:
dr hab. inż. **Marcin CHRZAN, prof. UTH** Wydział Transportu i Elektrotechniki – Uniwersytet Technologiczno - Humanistyczny w Radomiu, ul J. Malczewskiego 29, mail:m.chrzan@uthrad.pl
mgr inż. **Paweł Pirosz**, Zespół Szkół Elektronicznych w Radomiu, ul. Sadkowska 19, mail:pawelpirosz@elektronik.edu.pl