

LEWIŃSKI Andrzej, UKLEJA Paweł

ŁĄCZNOŚĆ BEZPRZEWODOWA POMIĘDZY SYSTEMAMI SRK NA LINIACH REGIONALNYCH

Streszczenie

Technologie bezprzewodowe są nowym kierunkiem w rozwoju systemów sterowania ruchem kolejowym na liniach regionalnych. Mimo transmisji otwartej są one tak samo bezpieczne jak dotychczas stosowane linie kablowe, czy światłowodowe. W pracy podjęto analizę zastosowania radiolinii do komunikacji pomiędzy systemami stacyjnymi srk stosowanymi na liniach regionalnych.

WSTĘP

Nowe technologie transmisji danych wypierają powoli stare opierające się na stałych łączach miedzianych lub światłowodowych. Wynika to z kilku czynników, do których należy zaliczyć przede wszystkim zalecany przez dyrektywy UE pro ekologiczny szynowy transport zbiorowy, ale też rozwój regionów związany głównie z turystyką oraz zapewnieniem dojazdu do centrów przemysłowych. Technologie bezprzewodowe, oparte głównie na publicznych sieciach telekomunikacyjnych ułatwiają dostęp do sieci wielu użytkownikom jednocześnie bez potrzeby budowy skomplikowanej infrastruktury kablowej. Dodatkowo umożliwiają łączność w trudno dostępnych miejscach lub tam gdzie nie opłaca się budować linii kablowych lub jest niemożliwe np. z powodów ekologicznych. W komputerowych urządzeniach sterowania ruchem kolejowym, gdzie transmisja danych odgrywa ważną rolę w bezpieczeństwie ruchu pociągów, podejmowane są pierwsze kroki wykorzystania łącz bezprzewodowych w komunikacji pomiędzy poszczególnymi elementami/systemami srk. Na uwagę zasługuje tu np. system ESTER firmy Kombud S.A. Radom.

1. OGÓLNA CHARAKTERYSTYKA BEZPRZEWODOWEJ TRANSMISJI DANYCH

Wytyczne dla transmisji danych zamieszczone są w normie EN 50159-2011. Zawiera ona dwie części: pierwszą odnoszącą się do zamkniętej transmisji danych i drugą dotyczącą otwartej transmisji danych. W koncepcjach łącz bezprzewodowych pomiędzy systemami srk brane jest pod uwagę zapewnienie bezpieczeństwa w sieciach otwartej transmisji danych takich jak: radiowe, Internet lub poprzez łącza współdzielone o publicznym dostępie [1], [2].

Ze względu na swoją budowę sieci bezprzewodowe narażone są w dużo większym stopniu na ingerencję. Sieć bezprzewodowa cechuje się rozgłaszaniem sygnału. Aby informacje przesyłane w bezprzewodowej sieci były poufne, trzeba je chronić poprzez szyfrowanie [7]. Ochrona przesyłanych informacji polega na zarządzaniu szczegółami ich szyfrowania i deszyfrowania. W rozpatrywanym przez autorów modelu bezpieczeństwo transmisji danych

opiera się na algorytmie AES z kluczem 256-bitowym. Na dzień dzisiejszy jest to jedno z najlepszych zabezpieczeń stosowanych w praktyce.

Algorytm AES (Rijndael) charakteryzują poniżej wymienione cechy [7]:

- ma charakter publiczny ,
- daje się łatwo zaimplementować zarówno w sposób sprzętowy jak i programowy,
- posiada dwa warianty: 128-bitowe bloki ze 128-bitowymi kluczami oraz 128-bitowe bloki z kluczami 256-bitowym,
- realizuje szyfrowanie blokowe w oparciu o klucz symetryczny.

Z matematycznego punktu widzenia algorytm Rijndael bazuje na teorii ciał Galois, co umożliwia formalne dowodzenie jego istotnych cech bezpieczeństwa. W praktyce stosuje się go w implementacjach języka C, bez żadnego odniesienia do matematyki [7].

Szyfrowanie odbywa się tutaj przez zastosowanie podstawień i permutacji w ramach wielokrotnych rund, które zależą od długości bloków i kluczy.

W systemach bezprzewodowych z bezpieczną transmisją danych używanych w kolejnictwie stosuje się, oprócz szyfrowania, dodatkowe mechanizmy zabezpieczające. Do tych mechanizmów należą [1],[2]:

- Numer sekwencyjny wiadomości
- Datowanie wiadomości
- Czas końca wiadomości
- Źródło identyfikatorów i przeznaczenia
- Komunikat zwrotny
- Procedury identyfikacji
- Kod bezpieczeństwa.

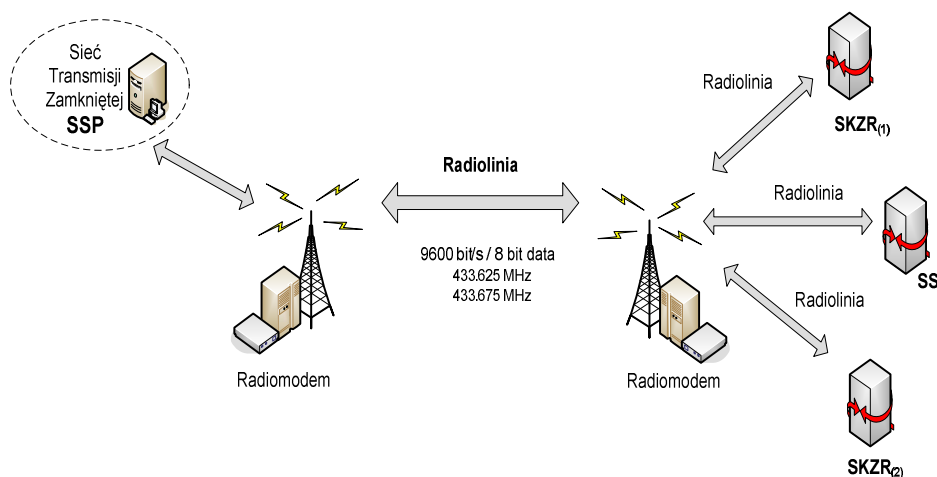
Mechanizmy te służą do wykluczenia zagrożeń typowych dla sieci bezprzewodowych takich jak: maskarada, wstawienie, powtórzenie, usunięcie, zmiana kolejności, czy opóźnienie [1],[2].

2. ZAŁOŻENIA OTWARTEJ SIECI ZALEŻNOŚCIOWEJ A POZIOM BEZPIECZEŃSTWA W SYSTEMACH SRK

Systemy sterowania ruchem kolejowym stosowane w kolejnictwie wykorzystujące do wymiany danych transmisję zamkniętą spełniają wymagania PN-EN 50128, PN-EN 50129 i PN-EN 50159-1. Z tego względu należy przyjąć, że poziom bezpieczeństwa SIL - 4 gwarantowany we wspomnianych systemach musi być co najmniej taki sam dla systemów z otwartą transmisją danych. Powyższe założenie zostało udowodnione dla blokady liniowej i urządzenia zdalnej kontroli systemu przejazdowego w [2]. Dokonane tam analizy i obliczenia potwierdzają utrzymanie wymaganego poziomu bezpieczeństwa w systemach z otwartą transmisją danych i potwierdzają one właściwy kierunek rozwoju systemów sterowania ruchem kolejowym [2].

Na tej podstawie autorzy stawiają tezę, że transmisję otwartą można zastosować do wymiany danych pomiędzy systemami stacijnymi srk jako kolejny krok ich rozwoju i uniezależnienie się od instalacji przewodowej.

Przykładem może tutaj być system transmisji otwartej oparty na radiolinii zapewniającej kontrolę autoryzacji dostępu zaproponowany przez firmę Kombud S.A. Radom [1] w urządzeniach samoczynnej sygnalizacji przejazdowej. Radiolinia jest tu wykorzystywana do transmisji danych pomiędzy kontenerem sterującym, znajdującym się w obrębie przejazdu kolejowego, a punktami oddziaływania w torze. Dzięki takiemu rozwiązaniu nie ma potrzeby budowy trasy kablowej między wspomnianymi elementami, co w dużym stopniu skraca czas zabudowy urządzeń i ułatwia późniejszą ich eksploatację.



Rys. 1. Struktura systemu SSP z transmisją otwartą [1],[6]

Tak, jak to zostało przedstawione na rys.1, dwukanałowa (dwustronna) transmisja otwarta została zastosowana do przesyłania informacji poprzez dedykowaną radiolinię 433 625/433 765 MHz pomiędzy Lokalnym Centrum Sterowania (SS), z którego kontrolowany jest ruch kolejowy na całym odcinku Radom Płd. -Tomaszów Maz. a Systemami Kontroli Niezajętości Torów (SKZR) i Systemami Sygnalizacji Przejazdowej (SSP). W obecnej fazie testowania systemu zastosowano dodatkowe kanały transmisji oparte o łącza światłowodowe.

W przedstawianej koncepcji tego systemu SSP ESTER zastosowano telegramy zgodnie z typem transmisji B0 [1],[6], a szyfrowanie odbywa się wg standardu AES z kluczem 128-bitowym.

3. KONCEPCJA ZASTOSOWANIA TRANSMISJI OTWARTEJ W STEROWANIU RUCHEM KOLEJOWYM NA LINIACH REGIONALNYCH

Linie regionalne mają tę specyfikę, że dostęp do infrastruktury kablowej jest znikomy, a budowa trasy kablowej wzdłuż całej linii lub na jej fragmencie ze względu na teren (bagna, góry, utrudnienia w budowie typowej infrastruktury z wykorzystaniem kabli miedziany lub światłowodów) skazuje na niepowodzenie.

Wpisując się w światowy trend przechodzenia na otwartą transmisję danych w branży kolejowej można zaproponować system łączności wykorzystujący radiolinię pomiędzy stacjami urządzeniami srk zabudowanymi na takiej linii.

Koncepcja przewiduje stosowanie łącza radiowego typu punkt – punkt pomiędzy sąsiadującymi ze sobą urządzeniami stacjami srk. Wykorzystywana do tej pory transmisja RS 232 zostaje przeniesiona z kabli w eter. Wspomniany typ transmisji nie wymaga dużej przepustowości. Wykorzystywana częstotliwość mieści się w pasmach licencjonowanych w zakresie 300kHz – 2,5GHz, co zwiększa znacznie zasięg takiego łącza. Oprócz standardowych zabezpieczeń stosowanych w otwartych sieciach transmisyjnych zakłada się tutaj szyfrowanie wg standardu AES z kluczem 256-bitowym w celu praktycznego wykluczenia nieautoryzowanej ingerencji w sieć zależnościową (blokady liniowej) zabudowanych urządzeń srk.

W sieciach bezprzewodowych, oprócz klasycznych parametrów niezawodnościowych, stosuje się parametr dotyczący dostępności łącza w ciągu roku. Stosowane na dzień dzisiejszy urządzenia zarządzające radioliniami gwarantują taką dostępność na poziomie 99,999%, co daje w praktyce brak połączenia w ciągu roku rzędu kilku minut. Taki czas braku komunikacji

między urządzeniami stacyjnymi zabudowywanymi na liniach regionalnych nie powoduje zakłóceń w ruchu pociągów ze względu na jego charakterystykę.

4. ANALIZA TRANSMISJI OTWARTEJ POMIĘDZY SYSTEMAMI STACYJNYMI SRK

Rozpatrywanie transmisji otwartej pomiędzy systemami stacyjnymi dotyczy urządzeń instalowanych na liniach regionalnych. Poziom bezpieczeństwa systemów zależnościowych jest tam taki sam jak tzw. dużych systemów. Odległości pomiędzy urządzeniami mieszczą się w granicach $l = \langle 5\text{km}, 15\text{km} \rangle$.

Podstawowym modelem wyjściowym badania jest ogólny model systemu transmisji otwartej w wersji bez naprawy z jednym kanałem transmisji informacji.

Niezawodność każdej transmisji w pojedynczym kanale transmisyjnym przyjęta jest na poziomie:

$$\lambda_N = 10^{-4} h^{-1} \quad (1)$$

co oznacza, że 1 bit może ulec przekłamaniu w ciągu 10 000 godzin transmisji. Dotyczy to również transmisji zamkniętej, przewodowej [2], [8]. Dlatego w każdym typie transmisji podstawowym zabezpieczeniem jest kontrola integralności danych poprzez kod CRC (ang. *Cyclic Redundancy Code*). Powszechnie stosowane zabezpieczenie 32 bitowym kodem CRC prowadzi do istotnego obniżenia poziomu prawdopodobieństwa P_{NT} wystąpienia niekontrolowanego (a więc niebezpiecznego) przekłamania bitu:

$$\lambda_{NT} = \lambda_N \cdot p_{UE} = \lambda_N \cdot 2^{-32} \quad (2)$$

gdzie λ_N jest intensywnością wszystkich uszkodzeń w kanale transmisyjnym, $p_{UE}=2^{-C}$ jest prawdopodobieństwem niewykrycia błędu (C – numer nadmiarowości bitowej). Dla kodu CRC32 wartość p_{UE} jest równa 2^{-32} . Zależność jest też prawdziwa dla prawdopodobieństwa wystąpienia błędu krytycznego p_{NT} , gdzie p_N jest prawdopodobieństwem przekłamania bitu (przyjmuje się wartości rzędu 10^{-4} - 10^{-5})

$$p_{NT} = p_N \cdot p_{UE} = p_N \cdot 2^{-32} \quad (3)$$

W przypadku podanego zabezpieczenia przesyłanych informacji kodem CRC32 wszystkie systemy kablowe nawet w przypadku pojedynczego kanału transmisji spełniają wymagania SIL4 dotyczącego dopuszczalnego poziomu wystąpienia błędu krytycznego określonego współczynnikiem THR (ang. *Tolerable Hazard Rate*) [2]. Dotyczy to również systemów z transmisją bezprzewodową, w tym wspomnianego systemu ESTER [2], [8].

Zastosowanie dwóch kanałów transmisji (na przykład w przyszłości GSM-R i WiFi/WiMax) powoduje znaczne zmniejszenie prawdopodobieństwa wystąpienia niekontrolowanego przekłamania transmisji:

$$p_{NT} = p_{NT1} p_{NT2} \quad (4)$$

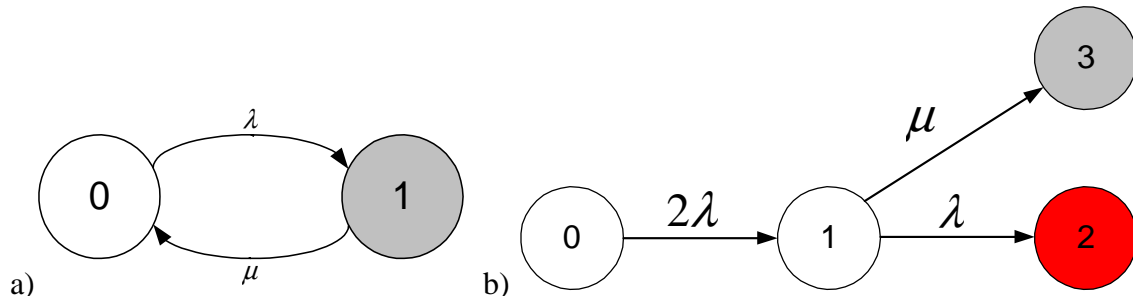
gdzie p_{NT1} i p_{NT2} są odpowiednio przekłamaniami niekontrolowanymi (niebezpiecznymi w obu kanałach. Przy identycznej strukturze obu kanałów (ten sam poziom P i to samo zabezpieczenie CR32) prawdopodobieństwo takiego błędu, a co za tym idzie wartość THR są o 3-4 rzędy wielkości mniejsze.

W przypadku transmisji bezprzewodowej poza bezpieczeństwem ważny jest również parametr dostępności (ang. *availability*) związany z utratą funkcjonalności systemu transmisji (przerwy w transmisji spowodowane zakłóceniami i zanikami).

Ponieważ rozpatrywana łączność odnosi się do systemów elektronicznych i programowalnych analiza modeli połączenia transmisji otwartej opiera się na procesach

jednorodnych i stacjonarnych Markowa [2], [3]. Wynika to z ogólnie przyjętego (również we wspomnianych normach EN) założenia o poissonowskim rozkładzie zdarzeń i związanym z tym wykładniczym rozkładzie czasu wystąpienia tych zdarzeń [2], [3]. (Dla uproszczenia przyjęto jednakowe charakterystyki niezawodnościowe i eksploatacyjne obu kanałów).

Dla podstawowego, jednokanałowego systemu transmisji, w tym też bezprzewodowej, sposób pracy przedstawia ogólny dwustanowy model z naprawą przedstawiony na rys.2a.



Rys. 2. Modele systemów transmisji a) ogólny model eksploatacji b) model bezpiecznego przełączania w transmisji dwukanałowej [2],[4]

Przejścia pomiędzy stanami uwzględniają:

- λ intensywność uszkodzeń
- μ odwrotność czasu powrotu ze stanu uszkodzenia.

odpowiada to typowym stanom pracy:

Stan 0 – transmisja danych bez usterek

Stan 1 – brak transmisji, powrót do stanu normalnej pracy.

Dostępność, określona jako graniczne prawdopodobieństwo przebywania w stanie 0 jest równa:

$$A = 1 - P_{1 \rightarrow \infty} = 1 - \frac{\lambda}{\lambda + \mu} \quad (5)$$

Do analizy niezawodnościowej transmisji otwartej przyjmuje się MTBF będący odwrotnością intensywności uszkodzeń (ang. *Mean time between Failures*) rzędu 100 lat (podawany przez producentów [2], [7], [8] na podstawie danych katalogowych).

W systemach transmisji kablowej parametr μ^{-1} odpowiadający faktycznej wartości czasu przerwy w transmisji jest rzędu 10 -100 ms, dla transmisji bezprzewodowej czas ten jest już mierzony w sekundach (1-10 s w zależności od rodzaju komunikującego się podsystemu typu licznik osi, blokady, nastawnica, ssp itp.). Jest to czas maksymalny, rzeczywiste badania prowadzą opóźnienia do poziomu 1-2 sekundy. Może to oznaczać stosunkowo dużą utratę funkcjonalności w stosunku do systemów tradycyjnych z transmisją zamkniętą, przy zapewnieniu tego samego poziomu bezpieczeństwa zgodnie ze standardami SIL. Jak widać w przypadku linii regionalnych nie stanowi to poważnego problemu, w związku ze stosunkowo małym ruchem pociągów (20 - 50 par pociągów na dobę) nie prowadzącym do zatrzymania ruchu wielu pociągów na szlaku. Pewnym rozwiązaniem może być zastosowanie w przyszłości alternatywnego kanału transmisji jakim może być powszechny dostęp do szerokopasmowego Internetu w standardzie WiFi/WiMax. Model bezpiecznej pracy dwukanałowego systemu transmisji przedstawia rys. 2.b. Poszczególne stany modelu opisują następujące sytuacje:

- Stan 0 - stan poprawnej pracy, równoległa transmisja,
- Stan 1 - system wykrył uszkodzenie transmisji w jednym kanale,
- Stan 2 - stan uszkodzenia niebezpiecznego, uszkodzone dwa kanały transmisji, brak reakcji bezpieczeństwa,

– Stan 3 (stan uszkodzenia kontrolowanego) - system wykrył uszkodzenie transmisji i rozpoczął reakcję bezpieczeństwa.

Parametr μ jest odwrotnością czasu reakcji na niezgodność informacji obu kanałach. Bezpieczeństwo wiąże się z granicznym prawdopodobieństwem osiągnięcia stanu krytycznego P2. Jest ono równe:

$$P_2 = P_2 \Big|_{t \rightarrow \infty} = \frac{\lambda}{\lambda + \mu} \quad (6)$$

Przyjmując wartość λ jak w jednokanałowym systemie transmisji, zaś wartość μ^{-1} na poziomie 100 ms wartość prawdopodobieństwa wystąpienia niekontrolowanego błędu systemu transmisji jest zgodna z wcześniejszymi oszacowaniami (3-4 rzędy wielkości mniejsza niż w przypadku transmisji jednokanałowej).

WNIOSKI

Ze względu na to, że systemy stacyjne mają poziom bezpieczeństwa SIL 4 wszelkie reakcje na usterki związane z transmisją danych pomiędzy nimi są realizowane w bezpiecznym oprogramowaniu systemów zależnościowych. Ma to istotny wpływ na czas wykrycia zarówno błędu niekrytycznego, jak i krytycznego, którego prawdopodobieństwo i intensywność wystąpienia regulują w sposób rygorystyczny normy UE.

Radiowa transmisja bezprzewodowa realizowana w oparciu o publiczne standardy (Internet, radiolinie) zapewnia ten sam poziom bezpieczeństwa, co tradycyjna transmisja przewodowa (skrętka miedziana, światłowód), aktualnie pewien problem stanowią procedury logowania się do sieci publicznych (GSM-R ma ten sam poziom opóźnień co standardowy GSM) co ogranicza gotowość, a więc dyspozycyjność takich systemów. Stanowi to problem w przypadku obciążonych szlaków (linie magistralne), ale w przypadku linii regionalnych obecnie kilkusekundowa utrata łączności (przy zapewnieniu wymaganego poziomu bezpieczeństwa) może dotyczyć jednego pociągu (w okresie 1-3 tygodni) co nie ma istotnego wpływu na prowadzenie ruchu pociągów zgodnie z rozkładem jazdy.

Niewątpliwie prowadzone prace nad rozwojem standardów bezprzewodowych (technologia LTE w systemach GSM czy kolejne wersje szybkich standardów WiFi/WiMax) mogą znacznie skrócić opóźnienia w transmisji bezprzewodowej.

Transmisja bezprzewodowa, oparta na publicznych standardach radiowych jest poważnym argumentem modernizacji linii regionalnych, zarówno z powodów ekonomicznych, ekologicznych i społecznych. Takie projekty są w większości finansowane ze środków UE, co dodatkowo aktywizuje rynek pracy i rozwój społeczności lokalnych

BIBLIOGRAFIA

1. A. Lewiński, L. Bester., A. Toruń: „*Sposoby realizacji transmisji otwartej w systemach sterowania ruchem kolejowym*”, Materiały konferencji LOGITRANS 2011, Politechnika Radomska 2011, Logistyka Nr 3/2011 (płyta CD)
2. A. Lewiński, T. Perzyński, A. Toruń: „*The Analysis of Open Transmission Standards in Railway Control and Management*”. Communications in Computer and Information Science 329), Springer-Verlag Berlin Heidelberg 2012),
3. Lewiński A.: „*Nowoczesne systemy telematyki kolejowej*”, Politechnika Radomska, Radom 2012
4. Lewiński A.: „*Problemy oprogramowania bezpiecznych systemów komputerowych w zastosowaniach transportu kolejowego*”, Monografie nr 49/2001, Politechnika Radomska, Radom, 2001

5. Lewiński A., Ukleja P.: „Bezpieczne sterowanie ruchem pociągów na liniach regionalnych”, Autobusy 3/2013, płyta CD
6. Perzyński T.: „Metoda tworzenia oprogramowania sterującego w systemach sterowania ruchem kolejowym”, rozprawa doktorska, Wydział Transportu, Politechnika Radomska, czerwiec 2009
7. Tannenbaum A., Wetherall D.: „Sieci komputerowe”, Wydanie V, Wydawnictwo Helion, Gliwice 2012
8. Materiały firmy Aprisa
9. Materiały firmy BOMBARDIER
10. Materiały firmy KOMBUD S.A

WIRELESS COMMUNICATION BETWEEN RAILWAY CONTROL SYSTEMS FOR REGIONAL LINES

Abstract

The wireless technology is a trend of railway control systems development especially designed for regional lines. The applied open transmission guarantees the same safety level such existing cable and optical connections. The paper deals with reliability analysis for radio-line applied for communication between interlocking systems for regional line

Autorzy:

prof. dr hab. inż. Andrzej Lewiński – Wydział Transportu i Elektrotechniki, Uniwersytet Technologiczno-Humanistyczny im. Kazimierza Pułaskiego

mgr inż. Paweł Ukleja - Scheidt & Bachmann Polska Sp. z o.o, ul. Wąska 15, 62-030 Luboń, tel. +48 (61) 894 60 13, Fax. +48 (61) 814 86 51, tel. kom. +48 668 173 196