Jacek Stępień, Jacek Kołodziej, Tadeusz Uhl, Jacek Blat

Analiza możliwości realizacji systemu sterowania kolejowego na podstawie publicznych sieci transmisyjnych w zgodności z zaleceniami normy PN-EN 50159

Systemy sterowania wykorzystywane na kolei realizują zarówno transmisję danych pomiędzy użytkownikami, jak również przekaz informacji kontrolno-sterujących między systemem centralnym (operatorem) i urządzeniami wykonawczymi. Ze względu na newralgiczność transmitowanych danych, systemy takie podlegają specjalnemu nadzorowi, a wiele odpowiednich norm opisuje zarówno zagrożenia na jakie narażone mogą być transmitowane informacje, jak i minimalne poziomy zabezpieczeń, które wymagane są w systemie. W artykule przedstawiona została analiza możliwości realizacji systemu sterowania wykorzystywanego na kolei, w oparciu o publiczne sieci transmisyjne.

W artykule opisano zagrożenia definiowane w normie PN-EN 50159 oraz metody zabezpieczenia przed nimi danych transmitowanych w publicznym internecie. Przedstawiono również propozycję ogólnej struktury systemu sterowania kolejowego, zbudowanego na podstawie protokołów TCP/IP.

Norma PN-EN 50159 definiuje zagrożenia jakim podlegać może transmisja sygnałów sterowania, wykorzystywanych w systemach kolejowych zarówno w systemach otwartych, jak i zamkniętych.

Przez system otwarty należy w tym przypadku rozumieć taki system, w którym mechanizm przekazu informacji wykorzystuje nieznane media transmisyjne (w tym publiczne – internet), współdzielone przez wielu użytkowników. Liczba użytkowników realizujących połączenia jest zmienna i nieznana oraz istnieje ryzyko nieautoryzowanego dostępu do danych.

W systemie takim wyodrębnić można trzy podstawowe elementy składowe:

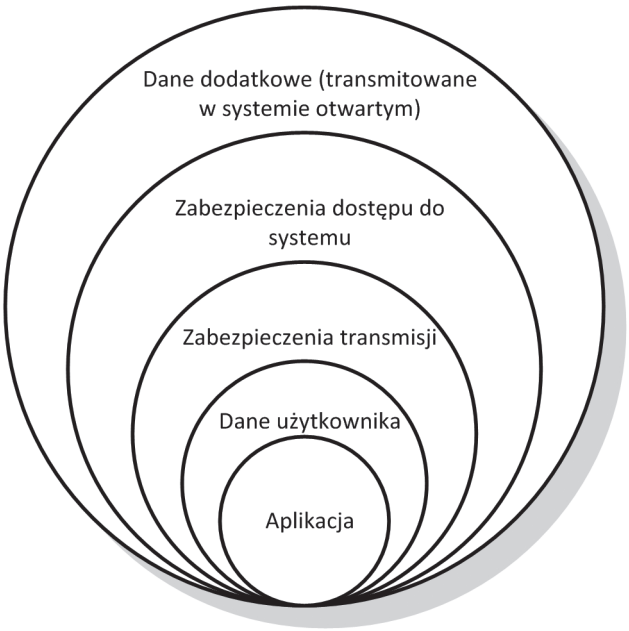
- urządzenia i układy transmisji danych,
- elementy pasywne – media transmisyjne,
- elementy systemowe umożliwiające routing transmisji – wieloetapową transmisję za pośrednictwem automatycznie (lub statycznie) konfigurowanych tras przesyłania informacji.

Strukturę systemu transmisyjnego przedstawiono na rysunku 1.

Dane transmitowane w systemie otwartym pochodzą zarówno z systemu sterowania, jak i od użytkowników „zewnętrznych" (niezwiązanych z systemem sterowania) i wykorzystują wspólne mechanizmy i media transmisyjne.

Zabezpieczeniu podlegać powinny dwa elementy:

- mechanizm przekazywania danych sterowania (protokół transmisji) – np. poprzez kodowanie czy szyfrowanie transmitowanych danych,
- dostęp do systemu transmisyjnego – realizowany poprzez autoryzację i autentyfikację użytkownika.



Rys. 1. Schemat struktury systemu otwartego

Norma precyzuje siedem głównych zagrożeń systemowych, którym podlegać może proces transmisji danych. Są to:

- powtórzenia,
- zagubienia,
- wtrącenia,
- zamiana kolejności transmitowanych danych,
- przekłamania,
- opóźnienia,
- maskarady.

Powtórzenia – to zagrożenie procesu transmisji, pojawiające się na skutek błędów przekazywania informacji, gdy do systemu sterowania dociera dwu lub kilkukrotnie (w różnych chwilach czasowych) ten sam komunikat. Istnieje zagrożenie niepotrzebnego, kolejnego wykonania tego samego rozkazu sterującego.

Zagubienia – czyli utrata komunikatu sterującego. Poza podstawową konsekwencją, jaką jest niezrealizowanie rozkazu sterującego, system źródłowy może nie być w stanie zweryfikować czy komunikat dotarł do systemu wykonawczego.

Wtrącenia – niektóre komunikaty sterujące mogą wymagać wcześniejszego wykonania innych, predefiniowanych sekwencji poleceń sterujących. Pojawienie się wskutek przekłamań transmisyjnych dodatkowego, nadmiarowego komunikatu sterującego może wpłynąć na przebieg sekwencji sterującej.

Zmiana kolejności transmitowanych danych – również w tym przypadku przebieg procesu sterującego może zostać zmieniony, szczególnie jeśli komunikaty sterujące muszą być wykonywane w określonej sekwencji.

Przekłamania – może okazać się, że zmiana jednego bitu w sekwencji sterującej spowoduje niepożądane, trudne do przewidzenia skutki. Należy podkreślić, iż same sekwencje sterowania nie muszą różnić się od siebie znacząco, natomiast efekt ich działania może być znacząco różny. Przekłamanie wskutek pojawienia się np. zakłócenia impulsowego w torze transmisji może wypaczyć sens komunikatu.

Opóźnienia – komunikaty, które wymagają procedur nadzoru czasu realizacji muszą podlegać procesowi sprawdzania czasu dostarczenia informacji (lub czasu jej wygenerowania), gdyż w przypadku opóźnień ich wykonanie może być niepożądane.

Maskarady – podszywanie się nieupoważnionych użytkowników (lub urządzeń spoza sieci) pod operatorów systemu sterowania, realizowane przede wszystkim za pośrednictwem ataków hakerskich.

Aby uniknąć tych zagrożeń lub je całkowicie wyeliminować, norma zaleca zastosowanie następujących mechanizmów zabezpieczeń:

- Autentyfikacja komunikatu – autoryzację nadawcy komunikatu (użytkownika i/lub urządzenia źródłowego).
- Weryfikacja poprawności struktury komunikatu – sprawdzenie, czy w procesie transmisji nie wystąpiły błędy i przekłamania sekwencji sterujących.
- Weryfikacja czasowa – określenie czasu ważności komunikatu oraz weryfikacja, czy nie został on przekroczony.
- Weryfikacja poprawności sekwencyjności transmisji – sprawdzenie, czy komunikaty docierają do systemu docelowego w kolejności generacji.

W celu realizacji wymienionych procedur zaleca się stosowanie:

- sekwencyjnego numerowania komunikatów,
- znaczników czasowych w komunikatach,
- procedur time-out'u – sprawdzania czasu transmisji,
- identyfikacji nadawcy i odbiorcy (urządzeń),
- zwrotnych komunikatów potwierdzeń poprawności transmisji,
- procedur identyfikacji użytkownika,
- kodów zabezpieczających,
- elementów kryptografii.

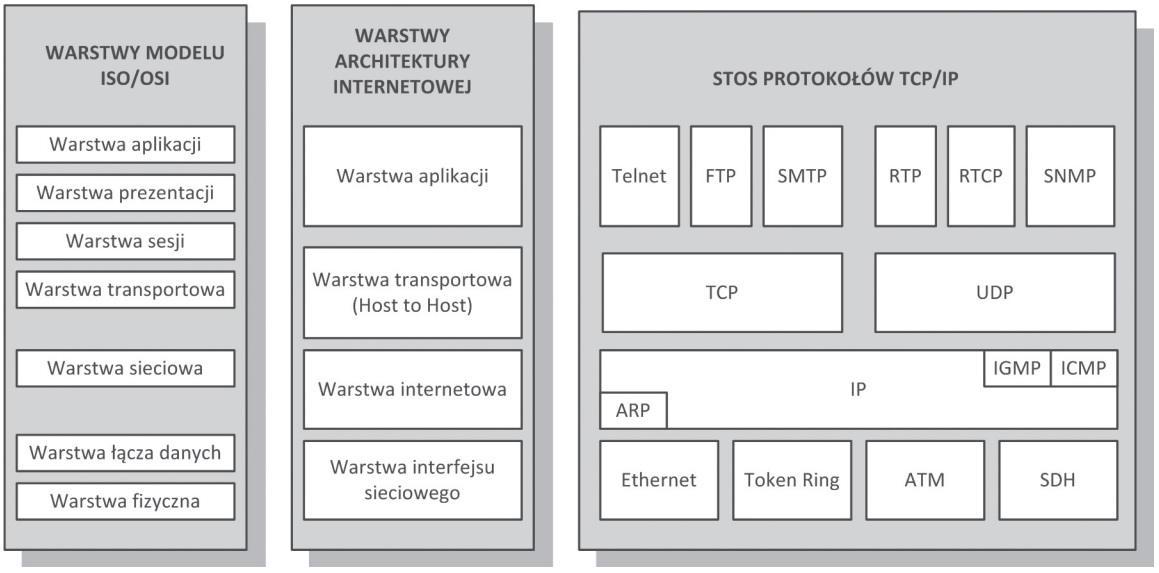
Ponadto nie sposób rozpatrywać normy PN-EN 50159 w separacji od innych dokumentów definiujących bądź opisujących zagrożenie w kolejowych systemach sterowania i definiujących mechanizmy przeciwdziałania, chodzi tu przede wszystkim o normy:

- PN 50128 – opisującą wymagania i zabezpieczenia oprogramowania sterującego,
- PN 50129 – definiującą zagrożenia bezpieczeństwa transmisji w systemach kolejowych i analizę stopnia ryzyka,

Wynika to chociażby z faktu, że szeroko rozumiany system otwarty to nie tylko elementy publicznego protokołu transmisyjnego, czy też elementów warstwy fizycznej opisującej właściwości toru transmisji danych. Wykorzystywane mechanizmy transmisji wynikają bezpośrednio z wymuszonych na poziomie aplikacji decyzji odnośnie np. wyboru protokołu warstwy transportowej, czy też metod zabezpieczania i kodowania informacji na poziomie warstwy aplikacji lub wynikającymi z uproszczonego modelu sieci komputerowych zgodnych z ISO/OSI (rys. 2). Są więc związane z zaleceniami odnośnie oprogramowania systemu sterowania.

Analiza możliwości realizacji systemu sterowania kolejowego na podstawie protokołów internetowych

Podstawowym systemem otwartym, wykorzystywanym do przenoszenia komunikatów w kolejowym systemie sterowania ma być



Rys. 2. Schemat struktury warstwowej sieci internet jako systemu otwartego

publiczna sieć internet. Pod tym pojęciem kryje się jednakże nie jeden protokół czy mechanizm transmisyjny, a cała ich rodzina [1]. Mówiąc o internecie jako systemie transmisji danych, najczęściej myślimy o protokołach i usługach, które nam oferuje, umożliwiając przekaz informacji.

Bezpośrednie mechanizmy transmisyjne opisywane są poprzez tzw. stos protokołów TCP/IP, na który składają się protokoły TCP (ang. *Transmission Control Protocol*) i UDP (ang. *User Datagram Protocol*) oraz IP (ang. *Internet Protocol*) [2, 5]. Definiują one podstawowe reguły implementacji protokołów warstwy trzeciej i czwartej, siedmiowarstwowego modelu ISO/OSI (ang. *International Standard Organization/Open System Interconnection*). W proces bezpośredniej transmisji „zaangażowane" są ponadto protokoły warstwy drugiej (w naszym przypadku jest to protokół Ethernet) oraz zalecenia implementacyjne warstwy fizycznej (pierwszej).

Protokoły internetowe wykorzystują jakby z natury, wiele mechanizmów wskazanych w normie PN-EN 50159, jako formę sugerowanych zabezpieczeń dla kolejowego systemu sterowania. Część z tych mechanizmów jest niezależnie implementowana w obu warstwach, co podnosi dodatkowo poziom bezpieczeństwa transmisji.

Sekwencyjne numerowanie komunikatów

Protokół TCP jest protokołem połączeniowym, wysyłającym i potwierdzającym sekwencyjnie pakiety. Teoretycznie rzecz biorąc nie występuje tutaj możliwość utraty pakietów, zatem nie jest wymagane numerowania pakietów, ale mimo to protokół implementuje mechanizm numeracji wysyłanych danych. 32-bitowy numer przypisywany jest każdemu transmitowanemu segmentowi danych i wykorzystywany w procedurach potwierdzeń.

Protokół UDP natomiast nie realizuje mechanizmu numeracji [5, 6].

Protokół IP stosuje 16-to bitowy numer sekwencyjny generowany przez nadawcę i transmitowany w nagłówku pakietu danych (datagramu). Wykorzystany może on zostać do realizacji przesłania do nadawcy komunikatu o błędzie transmisji.

Ponadto, zgodnie z normą PN-EN 50159, dla systemów sterowania ruchem kolejowym również warstwy wyższe muszą mieć wbudowaną funkcjonalność nadawania i kontrolowania numerów sekwencyjnych wysyłanych i odbieranych z systemów wykonawczych wiadomości. Z tego opisu wynika, że kontrola sekwencyjności przekazu informacji może być realizowana aż w trzech warstwach systemu transmisyjnego.

Znaczniki czasowe

Zdecydowanie ten element jest największym mankamentem protokołów internetowych. Z natury nie są one ukierunkowane na aplikacje czasu rzeczywistego i w podstawowym zestawie protokołów kwestie nadzoru czasowego są mocno ograniczone.

Protokół TCP nie jest wyposażony w mechanizmy wytwarzania, przesyłania czy kontroli znaczników czasowych.

W przypadku protokołu IP możliwe jest stosowanie znaczników czasowych przenoszonych w polach opcji nagłówka, pozwalających na określenie czasu emisji datagramu. Niestety nie jest to element, który w dokładny sposób zapewnia określenie czasu transmisji. Aby wymogi znaczników czasowych narzucanych przez normę zostały całkowicie wypełnione, należałoby zagwarantować dodatkowo pełną synchronizację zegarów w systemie (dla wszystkich urządzeń systemu sterowania). Ponieważ jest to czynnik dość newralgiczny, można byłoby pokusić się o rozbudowanie systemu sterowania o odpowiedni system dystrybucji czasu. Bezpośrednia realizacja wspólnego czasu w środowisku rozproszonym wymaga przesłania sygnału zegara do wszystkich współpracujących węzłów. W ostatnich kilku latach prowadzone są zaawanasowane prace nad systemami transferu czasu drogą radiową (satelitarne systemy GPS), światłowodową (np. OPTIME [7]) lub bazujące na klasycznych sieciach transmisji danych, dla których zdefiniowano protokoły takie, jak NTP/SNTP (ang. *Network Time Protocol/Simple Network Time Protocol*), PTP (ang. *Precise Time Protocol*) [8], *White Rabbit* [9].

W proponowanym systemie komunikację zapewniają internetowe protokoły pakietowe, dlatego naturalnym jest wykorzystanie do synchronizacji jednego z wymienionych protokołów. NTP oraz SNTP to protokoły służące do przekazywania informacji o czasie rzeczywistym z dokładności kilku milisekund [10]. W zastosowaniach do określania czasu rzeczywistego (data, godzina) są one wystarczające, gdy potrzeba jest precyzja synchronizacji zdarzeń na poziomie mikrosekund, możliwe jest zastosowanie metody White Rabbit (WR) lub protokołu PTP.

Rozwijanie technologii na podstawie aktywnej kompensacji propagacji pakietów w sieci Ethernet, stanowiącej trzon *White Rabbit*, znajduje się w fazie testowej i jest ciągle rozwijana przez społeczność naukową CERN. Sieć *White Rabbit* wymaga stosowania specjalnych urządzeń, które oprócz transferu czasu realizują także klasyczne usługi sieciowe. Standaryzowanym protokołem, który pozwala na uzyskanie mikrosekundowej dokładności jest protokół PTP. Został on zaprojektowany specjalnie na potrzeby do synchronizacji urządzeń w sieciach rozproszonych. Korzysta z wymiany komunikatów, które są przesyłane w sieci, jako pakiety danych, tym samym jego stosowanie nie jest ograniczone tylko do sieci Ethernet. Standardowe przełączniki Ethernet oraz routery wprowadzają zmienne w czasie opóźnienia pakietów, które limitują dokładność pomiaru czasu przejścia pakietu w zestawionej trasie. Co za tym idzie poprawa dystrybucji zegara narzuca wprowadzenie pewnych modyfikacji infrastruktury sieciowej, związanej z pomiarami opóźnienia i jego korekcją. Synchronizacja z mniejszą dokładnością może być osiągnięta drogą programową poprzez uśrednianie czasu propagacji pakietów. Chociaż PTP może być realizowany przez każdą sieć pakietową, to głównym celem jego dotychczasowego rozwoju było wykorzystanie protokołu UDP/ /IPv4 (ang. *User Datagram Protocol over Internet Protocol version 4*). Możliwe jest także synchronizowanie urządzeń serwerowych na poziomie usług oferowanych np. przez sieciowe funkcje systemu UNIX, pozwalające ma synchronizowanie zegara urządzeń komputerowych z zegarem serwera systemowego.

Po zapewnienie tej funkcjonalności możliwe staje się pełne i efektywne wykorzystanie znaczników czasowych protokołu IP oraz wprowadzenie mechanizmu dodatkowego – znacznika czasowego generacji komunikatu sterującego, na poziomie aplikacyjnym. Jako element zintegrowany z nagłówkiem komunikatu sterującego mógłby on zostać wykorzystany do wyznaczania czasu transmisji komunikatu oraz przez procedury określające jego ważność (procedury *time-out*).

Time-out

Protokół TCP wykorzystuje procedury *time-out* w celu weryfikacji poprawności dostarczenia pakietu danych do systemu docelowego. Parametr jest konfigurowalny (ustawiana jest jego wielkość) i definiuje czas, po którym system źródłowy powinien uzyskać pozytywne potwierdzenie odebrania pakietu od systemu docelowego. Po przekroczeniu tego czasu pakiet jest retransmitowany.

Mechanizm ten może okazać się niezwykle efektywny w proponowanym systemie, przy zastosowaniu wąskiego „okna potwierdzeń", wymuszającego indywidualne potwierdzanie każdego przesyłanego segmentu danych. Ponieważ komunikaty sterujące są informacjami krótkimi (mieszczącymi się w pojedynczym segmencie), potwierdzenie poprawnego dostarczenia segmentu będzie jednoznaczne z potwierdzeniem dostarczenia komunikatu sterującego w kolejowym systemie sterowania.

Ponadto, jeśli stworzone zostałyby mechanizmy generacji znaczników czasowych opisane w poprzednim podpunkcie, to oczywiście należałoby wprowadzić dodatkowy element *time-out* na poziomie aplikacji sterującej.

Identyfikacja nadawcy i odbiorcy

Protokół TCP wykorzystuje tzw. numer portu, jako element wspierający identyfikację źródła pakietu. Jest to numer identyfikujący aplikację, generującą transmitowany pakiet. Wprowadzenie unikatowego numeru portu dla aplikacji sterowania w połączeniu z mechanizmami adresacji warstw niższych stanowić będzie skojarzenie przesyłanego komunikatu nie tylko z konkretnym urządzeniem sterującym, lecz również aplikacją zarządzającą, umożliwiając rozbudowę systemu.

Protokół IP stosuje podczas przesyłania pakietów 32-bitowy adres nadawcy i odbiorcy. Wykorzystywane jest w przesłaniach wieloetapowych (jako element routingu pakietów). Jest unikatowy w skali globalnej i jednoznacznie określa urządzenia. W połączeniu z numerem portu z protokołu TCP stanowi o unikatowości w skali globalnej transmitowanego komunikatu.

Protokół Ethernet wykorzystuje podczas bezpośrednich transmisji (między elementami sieci lokalnej) 48-bitowy, unikatowy w skali globalnej adres MAC urządzenia źródłowego i docelowego. Jednoznacznie identyfikuje urządzenie lub jego element (kartę sieciową) generującą i odbierającą ramki danych.

Norma PN-EN 50159 zawiera również uwagę dotyczącą zapewnienia w systemie transmisji grupowych (skierowanych do wielu użytkowników systemu). System adresacji wykorzystywany przez protokoły warstw II i III umożliwia takie transmisje.

Protokół IP umożliwia realizację tzw. ukierunkowanych transmisji broadcastowych (rozgłoszeniowych) – pakiet danych transmitowany jest do docelowej sieci lokalnej, a tam rozgłaszany do wszystkich urządzeń w niej zainstalowanych. Ponadto możliwe jest zdefiniowanie grup adresów (tzw. multicast) odbiorców, którzy zakwalifikowani do grupy otrzymywać będą te same pakiety danych, co inni członkowie grupy (niezależnie od tego czy znajdują się w jednej sieci lokalnej, czy też w różnych punktach internetu).

Podobne możliwości w obrębie sieci lokalnej zapewnia Ethernet – możliwa jest transmisja ramek do wszystkich urządzeń w sieci lokalnej, jak również transmisje do grupy użytkowników. Niektóre urządzenia (karty) sieciowe wspierają ponadto dodatkową formę transmisji grupowych (ang. *Hash Addressing Mode*). Adresy grupowe użytkowników wyznaczane są w takim przypadku poprzez operacje logiczno-arytmetyczne, w których wykorzystywany jest adres MAC urządzenia, pozwalając na dodatkowe zabezpieczenie grupy użytkowników.

Kody zabezpieczające

W protokołach transmisyjnych internetu nie stosuje się redundancyjnych kodów zabezpieczających transmisję danych. Jako formę zabezpieczenia transmisji wykorzystywane są:

- protokół TCP – suma kontrolna dla nagłówka segmentu;
- protokół IP – suma kontrolna dla nagłówka datagramu;
- Ethernet – suma kontrolna dla całej transmitowanej ramki (nagłówek wraz z polem danych użytkownika); warstwa ta realizuje ponadto proces kodowania transmitowanych bitów w celu zapewnienie optymalności procesu transmisji danych; jeśli do transmisji wykorzystywane będą urządzenia *Fast Ethernet*, to ten konkretny protokół wykorzystuje kodowanie nadmiarowe 4B/5B, przy czym należy nadmienić, że nie jest on wykorzystywany do autokorekcji, a jedynie do dopasowania transmisji do wymogów toru przekazu informacji (ograniczenie pasma częstotliwościowego transmisji);
- kodowania nadmiarowe stosowane są czasami przez układy transmisyjne realizujące funkcje warstwy fizycznej; modemy xDSL zabezpieczają transmisję (w trybie bezpiecznym) przy pomocy nadmiarowego kodowanie Red-Salomona.

Oczywiście warstwy wyższe mogą stosować mechanizmy kodowania nadmiarowego, jako dodatkowy element zabezpieczenia i weryfikacji poprawności procesu transmisji.

Kryptografia

Zalecenia normy PN-EN 50159 ograniczają się do określenia metod kodowania MD4, MD5, DES (ang. *Data Encryption Standard*) jako wskaźników minimalnego poziomu jakości, wykorzystywanych procesów szyfryzacji. Metody te stosowane były w internetowych aplikacjach, ale ponieważ okazały się zbyt mało bezpieczne, zastąpiono je nowymi, znacznie efektywniejszymi.

Obecnie aplikacje internetowe najczęściej wykorzystują kodowania:

- SHA-1 (ang. *Secure Hash Algorithm*) kodowanie skrótowe;
- AES – (ang. *Advanced Encryption Standard*) – symetryczny szyfr blokowy z 256-bitowym kluczem [11].

Protokoły transmisyjne warstw I, II, i III nie wykorzystują kryptografii. Zadanie to spoczywa na warstwie aplikacyjnej, która musi wprowadzić elementy szyfryzacji i deszyfryzacji podczas generacji i rozkodowania komunikatu sterującego. Możliwe jest również wykorzystanie (oferowanych w gamie usług internetowych) usług bezpiecznego przesyłania haseł w trybie klient serwer, jako elementu autoryzacji i autentyfikacji użytkownika.

Możliwe jest również wykorzystanie znanych i powszechnie stosowanych algorytmów podpisu elektronicznego, jako elementu składowego w procesie generacji wszystkich, bądź wybranych (np. alarmowych) komunikatów sterujących. Tak wygenerowana wiadomość nosiłaby znamiona autoryzowanej personalnie informacji i posiadała wszelkie cechy oficjalnego dokumentu

Aplikacje i dodatkowe usługi wspierające zabezpieczenie systemu otwartego

Poza przedstawionymi aspektami bezpieczeństwa, wbudowanymi w protokoły warstw transmisyjnych sieci internetowej, warto wspomnieć o dwóch dodatkowych usługach sieciowych wykorzy-

stywanych w tej sieci, które mogłyby okazać się bardzo przydatne w konstruowanym systemie.

Pierwszym jest sprzętowy (lub programowy) system tzw. zapory ogniowej (*firewall*) [12]. Jeśli potraktowalibyśmy system sterowania, jako element niezależny, stanowiący sieć wewnętrzną (intranet), który łączy się z publicznym internetem tylko jednopunktowo (pozostała część transmisji odbywa się wewnątrz intranetu), to urządzenie takie mogłoby znacząco podnieść poziom bezpieczeństwa systemu. Podniosłoby to przede wszystkim poziom zabezpieczenia przed niepowołanym, użyciem systemu, czyli przed atakami hakerskimi. Mechanizmy ograniczenia dostępu dla użytkowników oraz urządzeń (powiązanych z adresami sieciowymi czy też konkretnymi aplikacjami) są we współczesnym internecie bardzo mocno rozbudowane i efektywne. Urządzenia takie zwiększają ponadto bezpieczeństwo w dodatkowy sposób. W znaczącym stopniu eliminują możliwość zawirusowania komputerów systemu wewnętrznego, co mogłoby ograniczyć potencjalne przyczyny awarii.

Drugim rozwiązaniem są połączenia VPN (ang. *Virtual Private Network*) – Wirtualna Sieć Prywatna) [13]. Połączenia takie można opisać, jako tunel przez który przesyłane są dane (w ramach sieci prywatnej, pomiędzy klientami końcowymi), za pośrednictwem sieci publicznej. Węzły sieci publicznej są „przezroczyste" dla przesyłanych w ten sposób pakietów. Taki kanał transmisyjny może opcjonalnie kompresować lub szyfrować przesyłane dane, w celu zapewnienia lepszej jakości lub większego poziomu bezpieczeństwa. Określenie „wirtualna" oznacza, że sieć ta zdefiniowana jest jedynie, jako struktura logiczna, działająca w rzeczywistości w ramach sieci publicznej, w odróżnieniu od sieci prywatnej, która powstaje na bazie specjalnie dzierżawionych w tym celu łącz. Pomimo takiego mechanizmu działania stacje końcowe mogą korzystać z VPN dokładnie tak, jak gdyby istniało pomiędzy nimi fizyczne łącze prywatne. Wirtualne Sieci Prywatne charakteryzują się dość dużą efektywnością, nawet na słabych łączach (dzięki kompresji danych) oraz dużym poziomem bezpieczeństwa (ze względu na szyfrowanie). Zastosowanie, wyłącznie takiego typu połączenia z użytkownikami spoza sieci wewnętrznej zapewniłoby wysoki poziom bezpieczeństwa i praktycznie uniemożliwiłoby ataki hackerskie.

Przedstawiona analiza funkcjonalna dotyczy praktycznie wyłącznie stosu protokołów TCP/IP, wykorzystujących jako „medium transmisyjne" w sieci lokalnej sieć Ethernet. Wynika to z faktu, że wbudowane w te protokoły mechanizmy bezpieczeństwa transmisji praktycznie w całej rozciągłości spełniają wymogi normy PN-EN 50159. Konieczność korzystania z dodatkowych usług warstw wyższych jest stosunkowo niewielka i dzięki temu upraszcza aplikację użytkową.

Nie oznacza to oczywiście, że nie można korzystać z innych mechanizmów transmisyjnych. Protokół UDP, coraz powszechniej wykorzystywany w internecie nie ma zaimplementowanych mechanizmów inicjowania i zamykania połączeń oraz potwierdzania transmisji, charakterystycznych dla TCP. Teoretycznie fakt ten dyskryminuje go i ogranicza możliwości wykorzystania w aplikacjach kolejowych. A jednak to właśnie UDP jest obecnie wykorzystywane, jako podstawowy protokół np. transmisji multimedialnych (czyli silnie „czasorzeczywistych") w internecie. Wynika to z prostego faktu – bezpieczeństwo procesu transmisji oraz nadzorowanie wymogów czasowych zostało w tym przypadku przekazane aplikacji. To aplikacja realizująca transmisję inicjuje połączenia, rejestruje członków grupy adresowej, wprowadza znaczniki czasowe i nadzoruje wielkości opóźnień procesu transmisji. Aby to było możliwe, wykorzystywane są protokoły wspomagające typu: RTP-RTCP (ang. *Real Time Protocol-Real Time Control Protocol*) [14] lub RSVP (ang. *Resource Reservation Protocol*) [15]. Pierwsze z nich zajmują się nadzorem procesu transmisji w aplikacjach czasu rzeczywistego, czyli wrażliwych na opóźnienia, te drugie, szeroko pojętym zagwarantowaniem jakości usług (ang. QoS – *Quality of Service*) dla aplikacji – w tym przypadku zajmują się nadzorem poprawności transmisji, gwarancją dostępności procesu transmisji i niezmienności jej parametrów.

Aplikacje zbudowane na podstawie tych protokołów spełniają również wszelkie wymogi stawiane przez normę PN-EN 50159, z zastrzeżeniem jednakże, że praktycznie cały system bezpieczeństwa usytuowany jest w warstwie aplikacyjnej.

Propozycja realizacji systemu

Przedstawiona propozycja zakłada stworzenie pseudo-intranetowej struktury przekazu komunikatów sterujących. Kolejowy system sterowania zrealizowany jest na podstawie infrastruktury sieci lokalnej pracującej w standardzie Ethernet. Większość ruchu sterującego ograniczona jest do wewnątrzsieciowych komunikatów lokalnych i nie jest przekazywana do publicznego Internetu. Całość pracuje pod nadzorem i przy wykorzystaniu protokołów TCP/IP oraz dodatkowych mechanizmów autoryzacji i autentyfikacji użytkowników oferowanych w usługach internetowych oraz dodatkowych aplikacji kryptograficznych (kodowanie nadmiarowe i kryptografia).

Dostęp do sieci publicznej zrealizowany jest w postaci jednopunktowego połączenia, na którym jako separatory ruchu oraz elementy zabezpieczające umieszczone są: sprzętowy *firewall* oraz *router* z możliwościami tworzenia połączeń VPN.

Firewall filtruje i sprawdza przede wszystkim pakiety wchodzące do systemu z zewnątrz, zabezpieczając system przed atakami hakerskimi oraz wirusami.

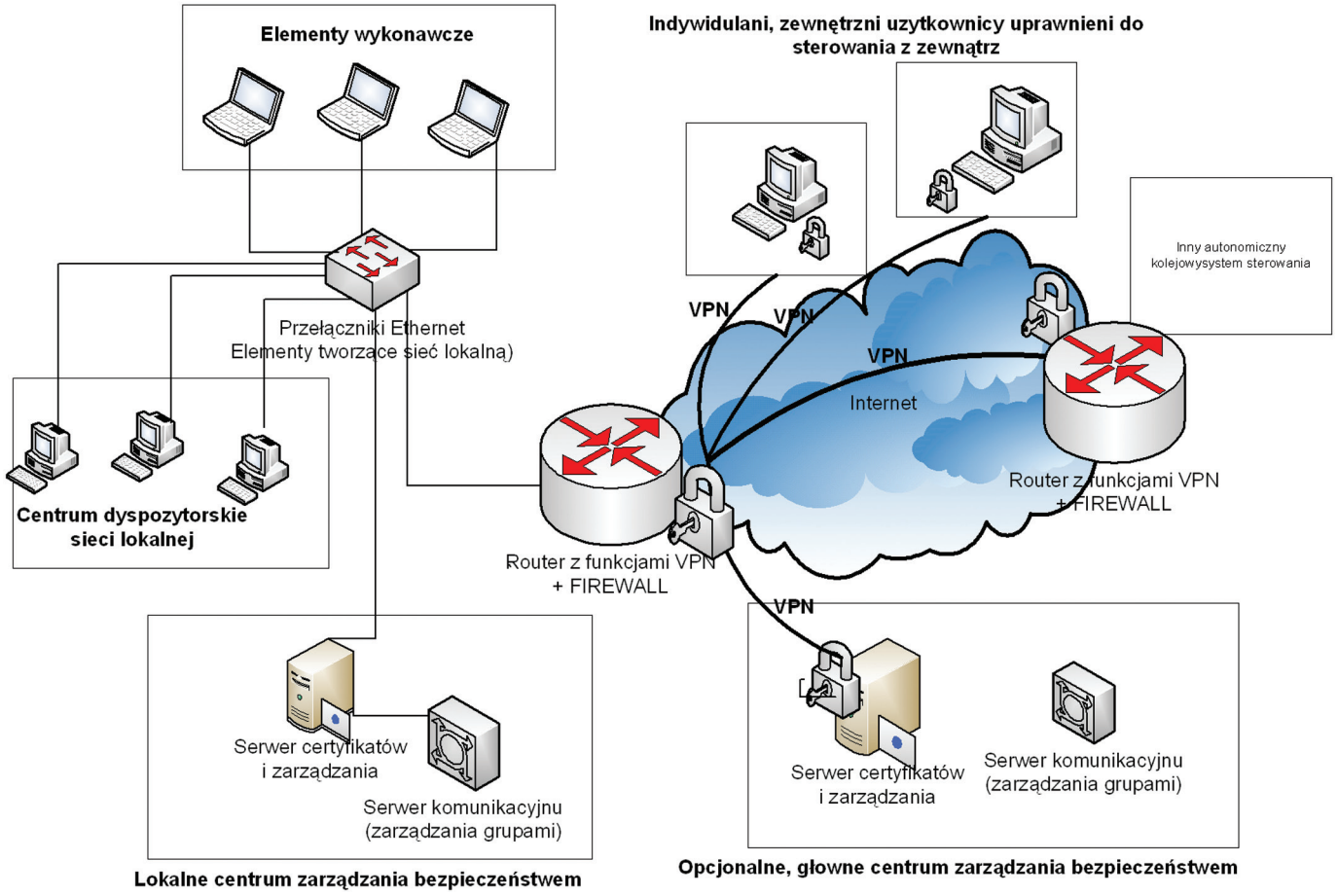
Każde zewnętrzne (autoryzowane) połączenie możliwe jest jedynie po stworzeniu indywidualnego połączenia VPN między *routerem* dostępowym a upoważnionym użytkownikiem z sieci publicznej.

Podobnie realizowane są połączenia z innymi systemami sterowania oraz opcjonalnym głównym systemem sterowania. W przypadku istnienia centralnego systemu zarządzania (z podległymi podsystemami sterowania kolejowego), to właśnie na tym systemie spoczywa obowiązek tworzenia i zarządzania grupami użytkowników oraz realizacji przydziału certyfikatów autentyczności i szyfrowania transmisji. Przykładową koncepcję stworzenia systemu sterowania kolejowego przedstawiono na rysunku 3.

Podsumowanie

Norma PN-EN 50159 definiuje zakres zagrożeń, jakim podlegać może transmisja danych w kolejowym systemie sterowania, zbudowanym w oparciu o otwarty system transmisji. Precyzuje jednocześnie zakres zabezpieczeń oraz metody ich zaimplementowania, które powinny zostać zrealizowane, aby wykluczyć (a raczej zminimalizować) te zagrożenia.

Z przedstawionej analizy wynika, że mechanizmy bezpieczeństwa wbudowane w protokoły komunikacyjne wykorzystywane



Rys. 3. Propozycja systemu sterowania opartego o sieć Ethernet i publiczny internet

w internecie odpowiadają lub przewyższają zalecenia normy PN-EN 50159.

Autentyfikacja komunikatu zrealizowana musi zostać jako element aplikacji sterowania i nadzoru. Wykorzystywać może zarówno wprowadzone w aplikacji znaczniki autoryzacyjne dla komunikatu sterującego, jak również adresy protokołów warstw II i III.

Weryfikacja poprawności struktury komunikatu przeprowadzana może być dwustopniowo – automatycznie przez protokoły sieciowe sprawdzające poprawność formy pakietu i poprawność sum CRC (warstwa II, III i IV stosu TCP/IP) oraz dodatkowo w warstwie aplikacji, bezpośrednio dla sekwencji sterującej.

Weryfikacja czasowa – na podstawie protokołów sieciowych wykorzystywać można wbudowane procedury *time out* protokołu TCP oraz znaczników czasowych protokołu IP. Dodatkowo w warstwie aplikacji, na podstawie usług oferowanych w sieciach iInternet należy zaimplementować funkcje automatycznej synchronizacji czasowej urządzeń w systemie oraz znaczników czasowych dla komunikatu.

Weryfikacja poprawności sekwencyjności transmisji – na poziomie warstwy IV realizuje to automatycznie protokół TCP, odtwarzając całość sekwencyjnie transmitowanej informacji. Automatycznie realizowane są również retransmisje w momencie zgubienia pakietu z sekwencji. Dodatkowo można wbudować w aplikację nadzór sekwencyjności komunikatów sterujących (zabezpieczający np. przed pojawieniem się bezpośrednio po sobie dwóch nawzajem wykluczających się poleceń systemowych). Ponadto protokoły transmisyjne, które wykorzystane mogą zostać do połączenia systemu sterowania z siecią internetową, zapewniają dodatkowe, bardzo rozbudowane pod względem bezpieczeństwa mechanizmy nadzoru i weryfikacji poprawności transmisji oraz uwierzytelniania użytkownika.

Narzędzia i usługi oferowane przez internet stwarzają ponadto stosunkowo szerokie możliwości konstrukcji systemu sterowania wymaganego typu i bezproblemowego wkomponowania go w sieć publiczną. To, jakie mechanizmy zostaną wykorzystane, zależy wyłącznie od poziomu zaawansowania aplikacji i systemu, a możliwości oferowanych usług na pewno są wystarczające, aby zapewnić zgodność systemu z normą PN-EN 50159.

Na podstawie przeprowadzonej analizy można stwierdzić, że budowa kolejowego systemu sterowania o strukturze:

- sieć lokalna w standardzie Ethernet, jako infrastruktura połączeń w sieci wewnętrznej między urządzeniami sterującymi a wykonawczymi;
- stos protokołów TCP/IP, jako element nadzorujący proces wymiany informacji między siecią wewnętrzną a siecią publiczną (internet);
- aplikacja sterowania rozbudowująca system zabezpieczeń o funkcjonalności znaczników czasowych oraz kryptografię;
- dodatkowe urządzenia separujące system od sieci publicznej i gwarantujące poufność transmisji w sieci publicznej (*router*, *firewall*);

zagwarantować może spełnienie wszystkich wymogów bezpieczeństwa stawianych przez normę PN-EN 50159.

❑

Literatura

[1] Comer D. E.: *Sieci komputerowe i intersieci*. WNT, Warszawa 2001
[2] Hall E.A.: *Internet Core Protocols*. O'Reilly, Sebastopol 2000.
[3] Stallings W.: *Data and Computer Communications*. Prentice Hall, 2007.
[4] *Internet Technical Resources* - http://www.cs.columbia.edu/~hgs/internet/
[5] *TCP/IP Tutorial and Technical Overview*. www.redbooks.ibm.com//pubs/pdfs/redbooks/gg243376.pdf
[6] *The TCP/IP Guide*. www.tcpipguide.com
[7] http://www.optime.org.pl/
[8] *Draft Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems*. IEEE Unapproved Draft Std P1588/D2.2, 2008.
[9] http://www.ohwr.org/projects/white-rabbit
[10] *IEEE Std. 1588 - 2002 IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems*. IEEE Std 1588-2002(2002).
[11] Schneier B.: *Kryptografia dla praktyków: protokoły, algorytmy i programy źródłowe w języku C*. WNT, Warszawa. 2002.
[12] Zwicky E., Cooper S., Chapman B.: *Building Internet Firewalls*. O'Reilly, 2009.
[13] Serafin M.: *Sieci VPN. Zdalna praca i bezpieczeństwo danych*. Helion, 2008.
[14] RFC 3550 – RTP: *A Transport Protocol for Real-Time Applications.*
[15] Naveen J.: *RSVP provides quality of service*. Network World, 2012.

Jacek Stępień
AGH Akademia Górniczo-Hutnicza w Krakowie
Wydział Informatyki, Elektroniki i Telekomunikacji
Katedra Elektroniki
jacek.stepien@agh.edu.pl

Jacek Kołodziej
AGH Akademia Górniczo-Hutnicza w Krakowie
Wydział Informatyki, Elektroniki i Telekomunikacji
Katedra Elektroniki

Tadeusz Uhl
AGH Akademia Górniczo-Hutnicza w Krakowie
Wydział Inżynierii Mechanicznej i Robotyki
Katedra Robotyki i Mechatroniki

Jacek Blat
Bombardier Transportation (ZWUS) Polska Sp. z o. o.
ul. Modelarska 12, 40-142 Katowice

Praca finansowana z projektu nt. „Innowacyjne rozwiązania sterowania ruchem i sygnalizacją dedykowane dla linii kolejowych małoobciążonych", finansowanego przez Narodowe Centrum Badań i Rozwoju nr 6 ZR9 2005 C/06688