Wybrane zagadnienia bezpieczeństwa transmisji informacji w systemach ITS

Siergiejczyk Mirosław, Korczak Daria

W artykule przestawiono istotę i zadania inteligentnych systemów transportowych, które stanowią szeroki zbiór różnorodnych technologii oraz technik zarządzania wykorzystywanych w transporcie. ITS pomagają w ochronie życia uczestników ruchu, ochronę zasobów środowiska naturalnego. Przy odpowiednim doborze parametrów oraz technologii łączności zwiększa się efektywność ITS.

Słowa kluczowe: inteligentne systemy transportowe, technologie informacyjne, bezpieczeństwo transmisji.

WSTĘP

Inteligentne Systemy Transportowe ITS (*Intelligent Transportation Systems*) to połączenie technologii informacyjnych i komunikacyjnych z infrastrukturą transportową i pojazdami w celu poprawy bezpieczeństwa, zwiększenia efektywności procesów transportowych oraz ochrony środowiska naturalnego. ITS wpływa na poprawę warunków podróżowania w zakresie multimodalnym – zajmując się prywatnymi i publicznymi środkami transportu drogowego, morskiego i lotniczego.

Systemy ITS mają za zadanie poprawiać efektywność sieci komunikacyjnej i zapewniać bezpieczeństwo uczestników ruchu. Zastosowanie ITS ma neutralny wpływ na środowisko naturalne. Wdrożenia Inteligentnych Systemów Transportowych w naszym kraju są coraz bardziej widoczne. Warszawa, Poznań i Olsztyn to tylko niektóre, już istniejące, przykłady „nowoczesnego" podejścia do rozwiązania problemów związanych z zatłoczeniem miast. Termin Inteligentne Systemy Transportowe oznacza szeroki zbiór różnorodnych technologii (telekomunikacyjnych, informatycznych, automatycznych i pomiarowych) oraz technik zarządzania stosowanych w transporcie w celu ochrony życia uczestników ruchu, zwiększenia efektywności systemu transportowego oraz ochrony zasobów środowiska naturalnego [1], [3], [9].

Kluczowym elementem systemów ITS jest informacja przesyłana za pomocą różnego typu środków łączności. Zastosowanie urządzeń telekomunikacyjnych i informatycznych sprawia, że systemy ITS są w rzeczywistości systemami teleinformatycznymi. Stąd też nabiera istotnego znaczenia problematyka bezpieczeństwa transmisji informacji pomiędzy elementami systemów ITS. W artykule zostaną zasygnalizowane tylko pewne aspekty tego problemu mające wpływ na architekturę systemu łączności (wymagane dodatkowe urządzenia służące do zapewnienia bezpieczeństwa przepływu danych).

1. ISTOTA I ZADANIA ITS

ITS oznacza systemy, które stanowią szeroki zbiór różnorodnych technologii (telekomunikacyjnych, informatycznych i sterowania, elektroniki) oraz technik zarządzania stosowanych w transporcie w celu ochrony życia uczestników ruchu, zwiększenia efektywności systemu transportowego oraz ochrony zasobów środowiska naturalnego.

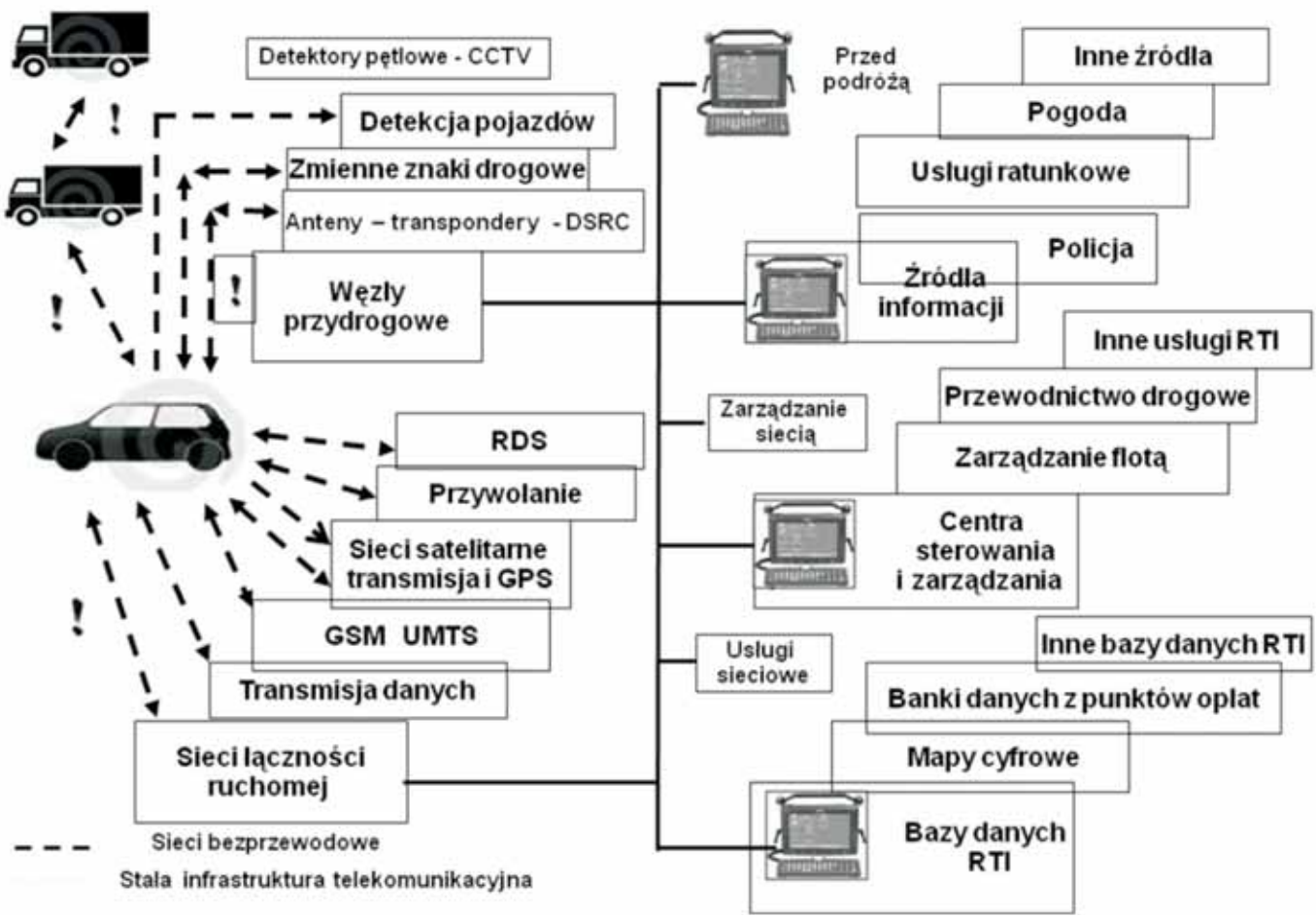
Przy doborze parametrów oraz technologii wykonania kanałów łączności trzeba uwzględniać też realizowane przez podsystemy zadania, oraz ich priorytet. Najwyższy priorytet powinny mieć połączenia realizowane przez systemy mające bezpośredni wpływ na bezpieczeństwo ludzi. Przy projektowaniu takich podsystemów i wyborze technologii trzeba szczególnie brać pod uwagę możliwość i niezawodność ich działania w sytuacjach kryzysowych i awaryjnych. Bardzo istotne są także połączenia mające wpływ na rozliczenia finansowe pomiędzy uczestnikami ruchu a administracją i właścicielem drogi. Przykładowe środowisko telekomunikacyjne ITS w transporcie drogowym zostało przedstawione na rysunku 1.

Istotą działania wszystkich systemów ITS jest podejmowanie decyzji na podstawie uzyskiwanych i dostępnych informacji. Trafność podejmowanych decyzji zależna jest od jakości dostępnych informacji, ich dokładności i aktualności. Należy zwrócić uwagę na fakt, ze wymagania na aktualność informacji, oraz skutki opóźnienia w ich przekazywaniu lub w związku z ich utratą, są różne w zależności od podsystemu. Opóźnienia w odczycie danych pogodowych w zasadzie w małym stopniu wpływają na działanie innych podsystemów. Natomiast opóźnienia w przekazywaniu informacji ratunkowych mogą skutkować utratą życia [9], 14].

Oczekuje się, że wdrożenie systemów ITS może wpłynąć na [14]:

- zwiększenie przepustowości sieci ulic,
- poprawienie bezpieczeństwa w ruchu drogowym,
- zmniejszenie czas podróży i zużycie energii,
- poprawienie jakości środowiska naturalnego (redukcja emisji spalin) i poprawienie komfortu podróżowania i warunków ruchu kierowców, podróżujących transportem zbiorowym oraz pieszych,
- redukowanie kosztów zarządzania taborem drogowym i związanych z utrzymaniem i renowacją nawierzchni.

Aby skutecznie realizować tego typu cele zarządzający systemem dróg powinien mieć dostęp do danych napływających automatycznie i w odpowiednim przedziale czasu. Niektóre dane muszą być dostępne w czasie rzeczywistym (np. alarmy, połączenia ratunkowe, obrazy z kamer). Inne dane mogą napływać z niewielkimi opóźnieniami. Część danych jest zbierana w urządzeniach i przekazywana dalej w określonych



Rys. 1. *Środowisko telekomunikacyjne ITS*

przedziałach czasu w postaci zagregowanej lub wstępnie przetworzonej Dane pobierane z klasycznych czujników niosą w sobie ograniczone zasoby informacyjne. W celu podejmowania adekwatnych decyzji zarządzający powinien mieć także możliwości weryfikacji napływających danych i podglądu sytuacji. Dlatego coraz częściej wprowadza się systemy wideo. Pozwalają one na monitorowanie newralgicznych punktów na żywo oraz dokumentowanie zdarzeń i podjętych działań [9].

Źle zaprojektowana sieć transmisji danych może uniemożliwić realizację celów stawianych przed systemem ITS. Budowa systemu ITS nie jest jednorazowym zadaniem ale procesem w czasie którego dodawane będą kolejne zadania i podsystemy. Ponadto ze względu na koszty, stan techniki, stan prawny itp. budowa kolejnych podsystemów będzie przesunięta w czasie, a systemy ITS będą eksploatowane przez dziesiątki lat. Powinno przewidywać się ich rozwój, a w szczególności gotowość systemów łączności do realizacji nowych zadań.

Każdy podsystem systemu ITS ma specyficzne wymagania na kanały łączności, które muszą być dobrane adekwatnie do potrzeb danego podsystemu, jego topologii, użytkowników, z uwzględnieniem kosztów zarówno budowy jak i eksploatacji systemu. Istotą działania wszystkich systemów ITS jest podejmowanie decyzji na podstawie uzyskiwanych i dostępnych informacji. Trafność podejmowanych decyzji zależna jest od jakości dostępnych informacji, ich dokładności i aktualności.

2. ZAGROŻENIA TRANSMISJI INFORMACJI W ITS

Kluczowym elementem systemów ITS jest informacja przesyłana za pomocą różnego typu środków łączności. Zastosowanie urządzeń telekomunikacyjnych i informatycznych sprawia, że systemy ITS są w rzeczywistości systemami teleinformatycznymi (najczęściej opartymi o protokół IP), które podatne są na te same zagrożenia [2], [4], [8], [11], [14]:

- przerwanie – jest atakiem prowadzącym do zerwania połączenia użytkownika z usługą ITS (np. call centre, witryna internetowa przedstawiającą stan warunków na drodze). Może to być np. przypadkowe lub celowe uszkodzenie fizyczne określonego elementu sieci (np. serwera, przewodu).
- przechwycenie – ma miejsce, gdy osoba niepowołana uzyskuje dostęp do zasobów sieci (np. podsłuch). Ten typ zagrożenia jest niebezpieczny jedynie poprzez fakt, iż atakujący uzyskuje dostęp do poufnych danych, jednak w porównaniu z innymi typami zagrożeń nie ingeruje w ich treść lub samo przesyłanie danych,
- modyfikacja – polega na zmodyfikowaniu danych przesyłanych przez użytkownika do systemu poprzez zmianę plików, wprowadzenie innych, nieprawdziwych danych.
- podrobienie – jest atakiem, który polega na podrobieniu przesyłanych danych. W tym przypadku intruz wprowadza nieprawdziwe dane. Mo-

dyfikacja i podrobienie są najbardziej niebezpiecznymi typami ataków ze względu na to, iż jeden intruz może wywołać dziesiątki, setki lub tysiące nieprawdziwych powiadomień o wypadkach, paraliżując pracę operatorów w CZR, podawać fałszywe dane dotyczące kursowania pojazdów komunikacji publicznej a także wskazywać błędne informacje na znakach zmiennej treści.

Wykorzystywane do budowy sieci rozwiązania i protokoły powinny być publicznie dostępne i otwarte. Połączenie oparte na protokole TCP/IP w sieciach publicznych lub w sieciach, które nie są w pełni kontrolowane przez użytkownika, stwarza poważne ryzyko. Sytuacja taka ma miejsce przede wszystkim wtedy gdy partnerzy komunikacyjni są połączeni ze sobą za pośrednictwem publicznego Internetu, jak w przypadku GPRS.

Po połączeniu sieci lub systemu komputerowego z zewnętrzną siecią pojawiają się zagrożenia w związku z [4], [7]:

- możliwością niekontrolowanego korzystania z wszelkich wewnątrzsieciowych usług i zasobów przez osoby trzecie,
- możliwością niekontrolowanego korzystania przez osoby trzecie z usług, które w zasadzie powinny być udostępniane wyłącznie wybranym zewnętrznym partnerom,
- możliwością manipulowania przepływem danych między podsystemami, partnerami przez osoby trzecie
- oraz możliwością przechwytywania przez osoby trzecie poufnych danych (np. haseł itp.) wymienianych między urządzeniami wchodzącymi w skład podsystemów ITS jak i pomiędzy systemem ITS i partnerami wykorzystującymi dane udostępniane przez podsystemy ITS.

Przedstawione powyżej zagrożenia mogą być istotnym czynnikiem wpływającym na bezpieczeństwo funkcjonowania systemu transportowego.

3. KONCEPCJA ZWIĘKSZENIA BEZPIECZEŃSTWA I NIEZAWODNOŚCI TRANSMISJI INFORMACJI W ITS

3.1. Wybrane problemy zapewnienia dostępności sieci

Podsystem telekomunikacyjny musi zostać wykonany przy założeniu zapewnienia redundancji systemu. Ma to na celu podniesienie niezawodności pracy Systemu ITS w sytuacji awarii jego podsystemów lub poszczególnych elementów. Wymagane jest takie zaplanowanie połączeń, aby awaria jednego węzła łączności lub urządzenia komunikacyjnego powodowała co najwyżej przerwę w przesyłaniu danych z tego węzła, ale nie stanowiła zagrożenia dla integralności całego systemu ITS.

Przy projektowaniu przebiegów światłowodów, w celu ograniczenia ilości niezbędnych do budowy podsystemu komunikacyjnego dla ITS włókien, należy stosować topologię budowy sieci w postaci pierścieni. W sieci szkieletowej powinny to być pierścienie (ringi) optyczne zapewniające połączenia alternatywne zarówno w przypadku pojedynczej awarii kabla (różne drogi kabli w pierścieniu), włókna jak i urządzenia aktywnego. W uzasadnionych przypadkach dopuszcza się topologię płaskiego ringu (ten sam kabel inne włókna) zapewniającą redundancję w przypadku awarii włókna i urządzeń przełączających.

Połączenia pomiędzy pierścieniami sieci dostępowej a sieci szkieletowej powinny być realizowane jako połączenia redundantne zapewniające redundancję w przypadku awarii pojedynczego urządzenia przełączającego w sieci oraz uszkodzenia pojedynczego włókna. Sieć łączności powinna posiadać możliwość łatwej rozbudowy o kolejne przyłącza i węzły sieci. Sieć łączności powinna [10]:

- umożliwiać przypisywanie i wykonywanie różnych priorytetów dla różnego rodzaju ruchu (*Quality of Service*),
- zapewniać separację podsystemów ITS od siebie przy jednoczesnym wspólnym wykorzystaniu zasobów sieci
- posiadać nadmiarowe włókna światłowodowe do wykorzystania w przyszłych zastosowaniach (minimum 50% włókien w przewodzie) lub do przełączenie w przypadku awarii włókna
- zapewniać szybką rekonfiguracje sieci w przypadku wystąpienia awarii możliwej do usunięcia przez rekonfigurację.

Z punktu widzenia zapewnienia ciągłości działania sieci transmisji informacji w systemach ITS istotnym zagadnieniem staje się również możliwość realizacji transmisji z wykorzystaniem dróg obejściowych. System powinien umożliwiać realizacje połączeń z określonym poziomem zabezpieczenia poprawności i pewności działania. Jedną z metod jest planowanie dróg obejściowych. W każdym przypadku powinno dążyć się do realizacji sieci redundantnej, Jednak koszty zapewnienia pełnej redundancji mogą być znaczące. Wobec czego wymagana jest analiza potrzeb i kosztów dla każdego z podsystemów ITS. Wtedy, gdy zbierane informacje mają niewielki wpływ na bieżące działanie systemu lub nie powodują zagrożenia życia można przyjąć metodę lokalnego backupowania danych i przechowywania ich do czasu przywrócenia łączności. Tam gdzie działają systemy związane z bezpieczeństwem należy dążyć do takiej konfiguracji sieci, aby była ona odporna na awarię pojedynczych połączeń, pojedynczych interfejsów lub urządzeń. Taka awaria nie powoduje odcięcia innych urządzeń lub węzłów. Dlatego też preferowana jest praca sieci łączności w topologii pierścieni.

Zapewnienie pracy w postaci pełnych pierścieni realizujących połączenia fizycznie różnymi drogami może być zbyt kosztowne do realizacji. Patrząc na mapę dróg w Polsce i topologię autostrad można przewidywać, że kolejne odcinki będą uzupełniały istniejącą infrastrukturę. Dlatego przy planowaniu połączeń backupowych należy uwzględniać przewidywany rozwój sieci.

Biorąc pod uwagę to, że typowa topologia wydzielonych sieci łączności ITS będzie pokrywała się na początku z przebiegiem autostrad to stosowana będzie praktycznie topologia pierścienia płaskiego, nie odporna na przecięcia kabla. Dlatego też można na końcach obsługiwanych przez taką sieć odcinków autostrad wykonywać dodatkowe połączenia do publicznej sieci transmisji danych, czyli sieci Internet. Połączenia takie mogą służyć jako dodatkowa, niezależna droga przekazywania kluczowych danych w przypadku awarii. Generalnie należy w każdym przypadku przeprowadzać analizę skutków awarii i przygotować działania do minimalizowania wpływu awarii na pracę systemu. Drogi obejściowe nie muszą zapewniać pełnej przepływności identycznej jak w sprawnym systemie – powinno to wynikać z ważności przekazywanych informacji i analizy kosztów. Najbardziej pożądane są automatyczne przełączania się systemu na drogi obejściowe. To wymaga zastosowania odpowiednich urządzeń, narzędzi i protokołów [3].

W związku z zagrożeniami wymienionymi powyżej należy podjąć odpowiednie środki bezpieczeństwa:

- tworzenie bezpiecznych kanałów transmisji,
- kontrola pobieranych i przekazywanych danych oraz ograniczanie dostępu tylko do wskazanych i niezbędnych danych dla partnerów,

- wzajemne uwierzytelnianie partnerów,
- zabezpieczanie integralności i poufności danych.

Ponieważ wymienione powyżej środki bezpieczeństwa muszą być stosowane nie tylko w podsystemie łączności (warstwa transportowa) ale i w warstwie aplikacji dlatego też w niniejszym dokumencie zostaną zasygnalizowane tylko pewne aspekty tego problemu mające wpływ na architekturę systemu łączności (wymagane dodatkowe urządzenia służące do zapewnienia bezpieczeństwa przepływu danych).

Przepływ danych między sieciami a systemami komputerowymi można kontrolować lub ograniczać stosując firewall na złączach pomiędzy pojedynczymi sieciami i podsieciami lub systemami komputerowymi. Programy firewall można tak skonfigurować, aby osoby trzecie nie miały dostępu do wewnątrzsieciowych usług i zasobów, a partnerzy zewnętrzni posiadali dostęp tylko i wyłącznie do przewidzianych dla nich usług.

W celu uwierzytelnienia partnerów oraz zapewnienia integralności oraz poufności danych należy użyć zaawansowanych zabezpieczeń. W tym celu można zastosować następujące technologie [4], [5], [6], [7], [12]:

- IPSec / Virtual Private Network (VPN)
- SecureShell (SSH)
- Secure Socket Layer (SSL) / Transport Layer Security(TLS)

Wymienione technologie powinny być stosowane przy przesyłaniu danych przez sieci publiczne lub przez sieci nie będące pod kontrolą administracji dróg krajowych i autostrad. Technologie te ingerują na różnych warstwach w przepływ danych w podobny sposób i mogą przy odpowiedniej konfiguracji zagwarantować wzajemne uwierzytelnienie oraz integralność i poufność danych.

3.2. IPSec / Virtual Private Network (VPN)

Zbiór protokołów IPSec umożliwia połączenie w sposób bezpieczny dwóch fizycznie nie połączonych sieci lub sieci i sytemu komputerowego przy wykorzystaniu sieci publicznej i bez wpływu na działanie aplikacji pracujących w tych sieciach. Na ogół obie strony używają routerów VPN, które po wzajemnym uwierzytelnieniu kodują cały przepływ danych pomiędzy tymi dwoma sieciami.

Ponieważ IPSec funkcjonuje w warstwie sieciowej, przez co umożliwia przepływ danych pomiędzy połączonymi sieciami, najczęściej instaluje się program firewall w celu ograniczenia i kontroli przepływu danych pomiędzy tymi sieciami lub systemami komputerowymi. Należy pamiętać, że środki bezpieczeństwa udostępnione przez IPSec obejmują wyłącznie przepływ danych pomiędzy dwiema połączonymi sieciami przez kanał utworzony w sieci publicznej, a przepływ danych w obrębie sieci połączonych kanałem nie podlega ochronie. Sama konfiguracja IPSec wiąże się z dużymi nakładami i sprawia problemy przede wszystkim, gdy używane są produkty różnych producentów oraz podczas korzystania z Internetu poprzez Network Adress Translation (NAT) [5], [11], [12].

IPSec (*Internet Protocol Security*), używany do realizacji bezpiecznych transmisji, to jeden z najbardziej skomplikowanych protokołów. Jego złożoność wynika z faktu, iż jest oparty na innych protokołach (AH, ESP, ISAKMP, IKE).

IPSec został rozwinięty przez IETF w celu zabezpieczenia TCP/IP na poziomie warstwy 3 modelu OSI, co pozwala uniknąć przypisywania IPSec do jednego konkretnego portu (tak jak np. 22 dla SSH czy 443 dla HTTPS). Inne znane bezpieczne protokoły, jak TLS/SSL czy SSH, zabezpieczają odpowiednio warstwy prezentacji i aplikacji w referencyjnym modelu OSI/ISO.

IPSec może być stosowany w połączeniach host-host, host-brama lub brama-brama. Pierwszy typ wymaga albo trybu transportowego, albo tunelowego, podczas gdy dwa pozostałe typy połączeń wymagają trybu tunelowego. Dzięki uwierzytelnianiu i szyfrowaniu pakietów IP, IPSec pozwala zabezpieczyć całkowicie transmisję danych opartą na TCP. IPSec pozwala na [6], [7]:

- Uwierzytelnianie. Ta funkcja oparta jest między innymi na koncepcji Cookiem oraz na kluczach wspólnych, adresach IP, nazwach pełnej (złożonej) domeny FQDN (*Fully Qualified Domain Name*), certyfikatach X.509,
- Integralność danych. Dzięki korzystaniu z algorytmów laszowania, możemy sprawdzać, czy dane zostały zmienione między punktem wysłania a punktem docelowym. Owa integralność oparta jest na dwóch głównych typach funkcji laszowania: MAC oraz HMAC,
- Niezaprzeczalność. Możliwość formalnej identyfikacji nadawcy w taki sposób, aby ten ostatni nie mógł zaprzeczyć, że jest autorem wiadomości. Ta opcja oparta jest na koncepcji podpisu cyfrowego,
- Poufność danych. Poprzez szyfrowanie, możemy sprawić, że nikt nie przeczyta naszych danych,
- Niemożność odtworzenia. Ta opcja realizowana jest przez mechanizm ochrony przeciw odtwarzaniu zaszyfrowanych danych PFS, który zostanie omówiony w dalszej części rozdziału.

Z wymienionych funkcji można korzystać poprzez używanie dwóch podprotokołów IPSec:

- AH (*Authentication Header*) – stworzony, aby zapewnić głównie integralność i uwierzytelnianie danych;
- ESP (*Encapsulating Security Payload*) – który zapewnia poufność poprzez kodowanie, a także ewentualnie uwierzytelnianie. ESP jest używany dużo częściej niż AH. W szczególnych przypadkach można wymusić użycie obydwu protokołów,
- IKE (*Internet Key Exchange*) v1 oraz v2 – dostarcza mechanizm współpracy między dwoma punktami połączenia, ustala dostępne protokoły bezpieczeństwa i określa które z nich będą używane.

Połączenie (tunel) IPSec oparte jest na wykorzystaniu jednokierunkowych systemów bezpieczeństwa (SA – *Security Association*) uprzednio ustanowionych między łączącymi się podmiotami. Parametry SA mogą być wpisywane ręcznie przez administratorów lub ustalane automatycznie z użyciem protokołu IKE (*Internet Key Exchange*). To, że system bezpieczeństwa jest jednokierunkowy oznacza, iż potrzeba dwóch SA na jedno połączenie – po jednym do wysyłania i odbierania informacji. Połączenie IPSec identyfikują trzy podstawowe cechy [6]:

- Wskaźnik parametrów bezpieczeństwa (SPI – *Security Parameters Index*). Jest to 32-bitowy łańcuch o znaczeniu lokalnym (właściwy dla systemu, który zarządza systemem bezpieczeństwa), przenoszony jawnie w nagłówkach AH oraz ESP. SPI o wartości 0 jest szczególnym przypadkiem oznaczającym, że żaden SA nie został jeszcze utworzony,
- Adres docelowy systemu docelowego lub urządzenia pośredniczącego (router, firewall),
- Identyfikator protokołu bezpieczeństwa (SPId – *Security Protocol Identifier*), który wskazuje na użyty podprotokół (AH lub ESP).

Dla każdego z użytych protokołów istnieje osobny SA i tak mamy IPSec SA, IKE SA. Ponadto, gdy zaangażowane są typy ESP oraz AH, będą konieczne dwa SA,

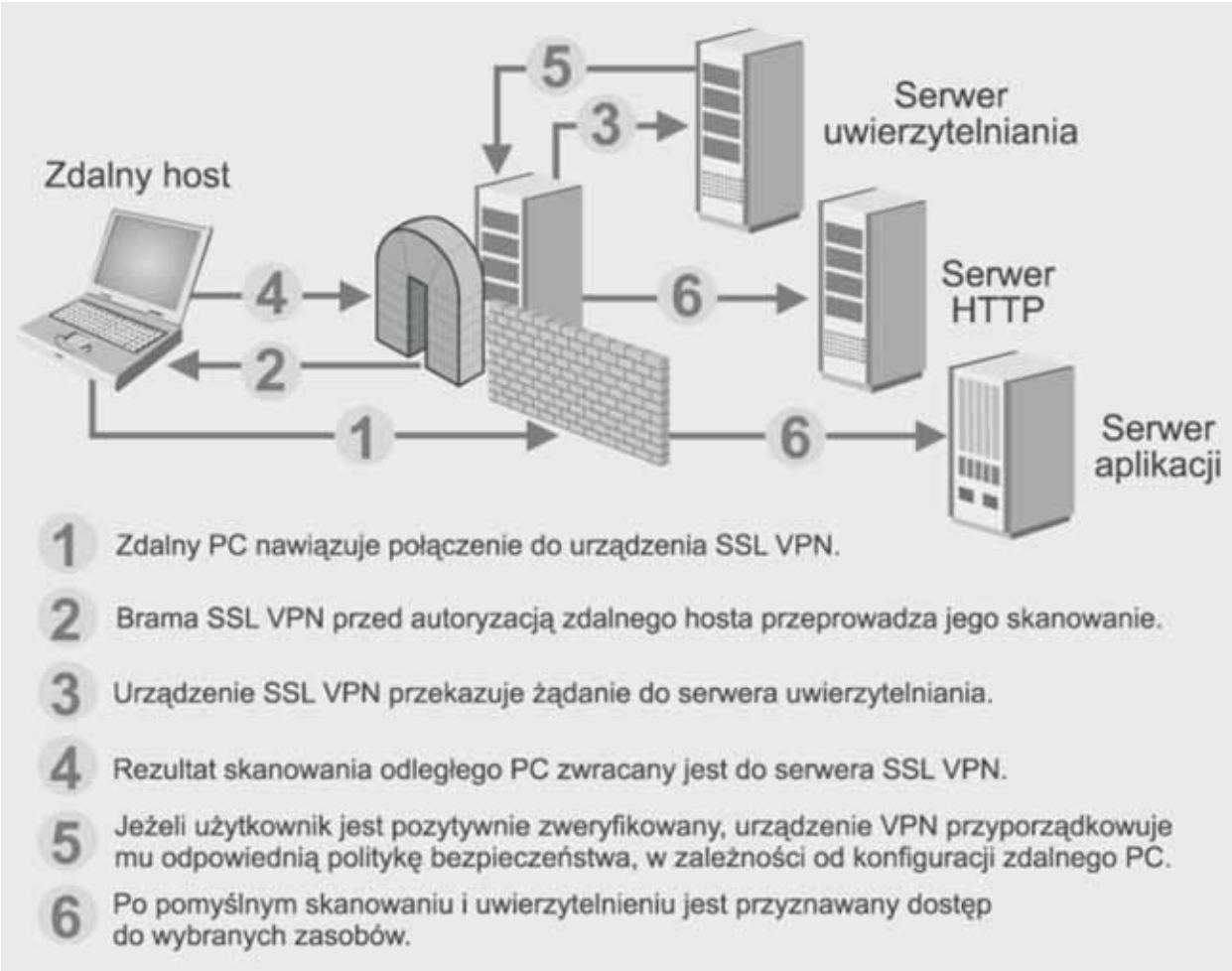
po jednym dla każdego typu. Jest to tak zwane zagnieżdżanie tuneli, przy czym najpierw zawsze musi być wykonany ESP, a po AH.

Każdy SA jest zawarty w bazie systemu bezpieczeństwa (SAD – Security Association Database). Baza ta zawiera odpowiednie informacje dla każdego SA, co pozwala na odpowiednie podejście do każdego pakietu, jaki będzie wysyłany. Jest to prosta baza danych, do której będzie się odwoływał SPD. Baza ta zawiera wszystkie informacje opisujące SA. Drugą bazą, którą definiuje się przy tworzeniu połączeń IPSec jest baza polityki bezpieczeństwa (SPD – *Security Policy Database*), która w przypadku każdego pakietu wchodzącego lub wychodzącego pozwoli zdecydować, czy spełnia on reguły bezpieczeństwa, a nawet, czy będzie upoważniony do przejścia.

3.3. SecureShell (SSH)

Protokół SSH jest jednym z tzw. protokołów zdalnej sesji. Oznacza to, że program korzystający z tego protokołu (często również o nazwie zawierającej skrót „SSH") umożliwia komunikację ze zdalnym komputerem. Przy pomocy SSH można więc poprzez sieć Internet zalogować się na się na odległym serwerze i pracować na nim tak, jak przy pomocy fizycznie podłączonego doń terminala. Inaczej jednak niż w przypadku protokołu Telnet, protokół SSH zapewnia szyfrowanie całej transmisji (łącznie z nazwą konta oraz hasłem, transmitowanym podczas sekwencji logowania się na serwerze). Protokół ten udostępniony początkowo w wersji 1 szybko ewoluował i aktualnie częściej używana jest jego 2-ga wersja. Oprogramowanie sieciowe zainstalowane na serwerze platon potrafi połączyć się z programem - klientem SSH przy pomocy obu wersji protokołu. Oczywiście, ze względu na liczne udoskonalenia włączone do wersji 2 protokołu, zalecane jest posługiwanie się tą właśnie wersją.

Zasada działania protokołu SSH opiera się na kryptograficznej technologii RSA i jest następująca: każdy z komputerów, na którym zainstalowane jest oprogramowanie SSH posiada parę kluczy: tzw. klucz prywatny dostępny tylko dla administratora komputera (i oczywiście oprogramowania systemowego obsługującego protokół SSH) oraz klucza publicznego dostępnego dla wszystkich użytkowników sieci. Klucze te są tak zbudowane, że informację zaszyfrowaną kluczem prywatnym można rozszyfrować tylko przy pomocy klucza publicznego i odwrotnie informację zaszyfrowaną kluczem publicznym można rozszyfrować wyłącznie przy pomocy klucza prywatnego. Klucze są więc ze sobą powiązane, ale żadnego z nich nie można odtworzyć na podstawie znajomości drugiego. Połączenie SSH inicjowane jest po stronie programu - klienta SSH. Klient łączy się z serwerem i otrzymuje od niego jego klucz publiczny. Klucz ten porównywany jest z zachowanym w wewnętrznej bazie danych klienta, z poprzednich połączeń. W przypadku wykrycia niezgodności kluczy wyświetlane jest specjalne ostrzeżenie umożliwiające przerwanie połączenia. Następnie, klient przekazuje serwerowi swój klucz



Rys. 2. *Schemat uzyskania dostępu do zasobów sieci SSL VPN [6]*

publiczny, generuje losową 256 bitową liczbę, szyfruje ją przy pomocy swojego klucza prywatnego oraz klucza publicznego serwera. Serwer po otrzymaniu tak zakodowanej liczby rozszyfrowuje ją przy pomocy swojego klucza prywatnego i klucza publicznego klienta. Tak otrzymana liczba jest losowa a ponadto znana tylko klientowi i serwerowi. Jest ona używana jako klucz do kodowania podczas dalszej komunikacji. SSH pozwala zabezpieczyć sieć przed atakami typu [2], [4]:

- IP spoofing,
- IP source routing,
- DNS spoofing,
- przechwycenie haseł użytkowników przesyłanych przez sieć w postaci jawnej,
- atakach opierających się na podsłuchu i zafałszowaniu autoryzacji na poziomie protokołu X-Windows.

SSH nie zabezpiecza jednak przed innego rodzaju atakami, w szczególności jeżeli włamywacz uzyska uprawnienia superużytkownika, może również manipulować danymi na których działa pakiet SSH. Wiele zdalnych usług, które wykorzystują protokół TCP/IP może być chronionych poprzez SSH. Między innymi: aplikacje użytkowników client-server, systemy baz danych i usługi takie jak HTTP, TELNET, POP, SMTP.

Używając SSH pamiętać należy, że przesyłanie połączenia do jakiegoś innego hosta, na którym nie jest otwarta sesja terminala, będzie kodowane tylko do hosta, na którym aktualnie odbywa się sesja terminala. Połączenie od tego hosta do hosta docelowego nie będzie kodowane. Docelowy host powinien więc zawsze być w bezpiecznej sieci lub być hostem na którym jest sesja terminala.

3.4. SSL(*Secure Socket Layer*)/TLS(*Transport Layer Security*) VPN

SSL (*Secure Socket Layer*) jest bezpiecznym protokołem transportowym, powszechnie wykorzystywanym do zapewnienia poufności i bezpieczeństwa transakcji np. w bankowości czy handlu elektronicznym. Często sieci SSL VPN nazywane są sieciami „bez klienta" (*clientless*), ponieważ większość przeglądarek internetowych obsługuje protokół SSL/TLS i właśnie one są wykorzystywane jako oprogramowanie klienta. Jest to przeciwieństwo rozwiązania opartego o IPSec, gdzie na każdym komputerze wykorzystującym zdalny dostęp musi być zainstalowane oprogramowanie klienckie dostarczone przez producenta. TLS (*Transport Layer Security*) jest protokołem warstwy transportowej opracownym przez IETF i zalecanym do używania w sieciach SSL VPN. Rozwiązanie SSL VPN standardowo oznacza zdalny dostęp do sieci poprzez bramę SSL VPN, lecz może również zawierać aplikacje obsługujące SSL np. klientów poczty (MS Outlook, Eudora) [6], [12].

SSL lub używany również TLS to protokóły, które działają w trybach połączeniowych, dzięki zastosowaniu protokołu TCP. Uproszczony schemat utworzenia sesji SSL ilustruje rysunek 2. Podobnie jak w IPSec istnieje tutaj faza wstępna, przed nawiązaniem połączenia, w której negocjowanych i weryfikowanych jest kilka parametrów:

- uwierzytelnienie serwera przez klienta za pomocą certyfikatów cyfrowych,
- opcjonalne uwierzytelnienie klienta przez serwer za pomocą certyfikatów cyfrowych (lub innych metod),
- bezpieczne wygenerowanie kluczy sesji, wykorzystywanych do szyfrowania i sprawdzania integralności danych.

SSL może wykorzystywać większość popularnych algorytmów generowania kluczy publicznych (RSA, DSA), symetrycznych (DES, 3DES, RC4) oraz algorytmów integralności danych (MD5, SHA-1). Istotną cechą SSL VPN jest to, że nie tworzy się otwartego tunelu do sieci firmowej. Polityka bezpieczeństwa jest wymuszana dla każdego połączenia, umożliwiając dostęp jedynie do określonych zasobów, w zależności od użytkownika, zdalnego urządzenia i jego lokalizacji. Podobnie jak w regułach stosowanych w zaporze ogniowej wszystko jest domyślnie zabronione, chyba że zostało wyraźnie udostępnione przez administratora. Systemy SSL VPN oferują szereg mechanizmów zabezpieczeń, które umożliwiają m.in. [6]:

- Uwierzytelnianie użytkowników – np. poprzez tokeny i hasła dynamiczne,
- Kontrolę dostępu użytkowników do określonych aplikacji systemu informatycznego,
- Weryfikację stanu bezpieczeństwa zdalnego komputera – np. poprzez sprawdzenie aktualności bazy skanera antywirusowego, obecności ściany ogniowej lub także niekiedy poprzez uruchomienie skryptu ActiveX, który pozwala wykryć uruchomione niebezpieczne oprogramowanie,
- Usuwanie danych aplikacji z komputera po zakończeniu pracy użytkownika – np. usuwanie zapisów w pamięci podręcznej przeglądarki Web,
- Rejestrowanie i raportowanie zdarzeń.

Rozwiązania SSL VPN oferują na ogół przynajmniej dwa z trzech poniższych mechanizmy dostępu [6]:

- Proxy – metoda podstawowa udostępniająca możliwość korzystania z aplikacji opartych o interfejs WWW, serwery plików oraz w zależności od rozwiązania inne aplikacje, takie jak poczta czy terminal znakowy. Do jej realizacji po stronie klienta wystarczy dowolna przeglądarka internetowa.
- Tunelowanie portów – wymaga uruchomienia po stronie klienta apletu lub aplikacji, która przekieruje połączenia sieciowe (na ogół tylko TCP) poprzez tunel SSL do urządzenia realizującego SSL VPN, a następnie do serwera docelowego. Można w ten sposób udostępniać w zasadzie dowolne aplikacje klient/serwer wykorzystujące statyczne porty TCP. Przykład zestawionej tym mechanizmem sesji przedstawia rysunek 3.20.
- Wirtualne interfejsy – metoda będąca ekwiwalentem IPSec lub RAS, polegająca na stworzeniu wirtualnego interfejsu sieciowego, przez który może być przekierowana cała komunikacja do i z sieci korporacyjnej. Metoda ta wymaga niestety uprawnień administratora systemu na używanym komputerze.

Połączenie tych mechanizmów zapewnia taką samą elastyczność jak sieciowe mechanizmy dostępowe takie jak RAS czy IPSec VPN. SSL VPN można wykorzystać z dowolnego miejsca, a w zasadzie z dowolnego komputera. Wystarczy do tego przeglądarka internetowa, która obsługuje tunelowanie SSL. Oczywiście pozostałe dwa mechanizmy dostępu wymagają uruchomienia dodatkowych programów, jednak zawsze może to się odbywać z poziomu przeglądarki oraz w przypadku tunelowania portów, w zasadzie nie ma żadnych wymagań w stosunku do konfiguracji stacji klienta (wystarczy wirtualna maszyna Javy). Należy też pamiętać, że cała komunikacja tunelowana jest w protokole SSL (pracujący na porcie TCP/443), który jest prawie zawsze dopuszczalnym przez politykę bezpieczeństwa sposobem komunikacji, natomiast IPSec znacznie rzadziej jest dozwolonym sposobem transmisji.

Istnieją dwa sposoby wdrożenia zdalnego dostępu z wykorzystaniem protokółu SSL. W pierwszym przypadku poszczególne serwery wykorzystując oprogramowanie SSL samodzielnie terminują tunele zestawiane przez zdalnych użytkowników. Alternatywą dla takiego

rozwiązania jest brama VPN, która z jednej strony stanowi interfejs terminujący tunele VPN zdalnych użytkowników, komunikując się jednocześnie z wewnętrznym serwerem w jego rodzimym formacie.

PODSUMOWANIE

IPSec dzięki wysokiemu poziomowi bezpieczeństwa, skalowalności i elastyczności zyskał sobie spore uznanie i miano najpopularniejszej metody tworzenia sieci VPN w sieciach IP. Stał się również gwarantem bezpieczeństwa w IPv6. Niemniej jednak zalety IPSec okupione są dużym jego skomplikowaniem, a im bardziej skomplikowany protokół, tym więcej trzeba złożonego kodu do jego implementacji. W konsekwencji łatwiej jest popełnić błędy programistyczne prowadzące do luk pozwalających na atak na sam system operacyjny. Poza tym trudno jest zrozumieć protokół i go zaimplementować poprawnie, co bezpośrednio prowadzi do niezgodności miedzy poszczególnymi implementacjami różnych producentów, a pośrednio może prowadzić do dodatkowych błędów. Także wdrożenie i utrzymanie sieci VPN bazującej na tym protokole wymaga od administratora bardzo dobrej znajomości protokołów składowych IPSec. SSL VPN jest relatywnie nową techniką zdalnego dostępu i wydaje się najlepszą metodą dostępową dla zdalnych i mobilnych pracowników. Nie można jednak całkowicie odrzucać pozostałych technologii i wybór rozwiązania oprzeć na specyficznych wymaganiach firmy.

W pracach dotyczących transmisji informacji w ITS należy zdefiniować interfejsy pomiędzy urządzeniami łączności (siecią łączności), a pozostałymi urządzeniami ITS. Należy wybrać takie interfejsy, które są dobrze zdefiniowane, popularne oraz tanie. Pozwoli to na stosowanie identycznych interfejsów w urządzeniach ITS, niezależnie od dostępnej sieci komunikacyjnej i stosowanych w niej urządzeń. Standaryzacja interfejsów umożliwi dołączanie dowolnych podsystemów do urządzeń sieciowych w sieciach łączności dedykowanych dla systemów ITS oraz ułatwi wybór i zmianę operatorów telekomunikacyjnych w przypadku korzystania z ich usług. Ważnym problemem jest też, zgodnie z [13], zapewnienie ciągłości usług ITS, czyli zdolności do zapewnienia nieprzerwanych usług w ramach sieci transportowych na obszarze Unii Europejskiej oraz zapewniania interoperacyjności, tak aby ITS oraz procesy gospodarcze będące ich podstawą były zdolne do wymiany danych, informacji i wiedzy, aby umożliwić skuteczne świadczenie usług ITS.

BIBLIOGRAFIA

1. Chowdhury M. A., Sadek A.: *Fundamentals of Intelligent Transportation Systems Planning*. Artech House ITS Library. Boston, London 2003.
2. Karpiński M.: *Bezpieczeństwo informacji*. Wydawnictwo: W.PAK 2012.
3. Klein L.A.: *Sensor Technologies and date requirements if ITS. Artech Hause*, ITS Library, 2001.
4. Liderman K.: *Bezpieczeństwo informacyjne*. Wydawnictwo Naukowe PWN, Warszawa 2012.
5. Nader J.C.: *VPNs Illustrated: Tunnels, VPNs, and IPSec*, Addison Wesley Professional 2005.
6. Ryłko K.: *Rozwiązania SSL VPN*. Networld 09/2005. IDG Warszawa 2005
7. Serafin M.: *Sieci VPN. Zdalna praca i bezpieczeństwo danych*. Helion, Gliwice 2009.
8. Siergiejczyk M.: *Zagadnienia realizacji wirtualnych sieci prywatnych dla spółek kolejowych*. Logistyka nr 3/2009. Poznań 2009.
9. Siergiejczyk M.: *Efektywność eksploatacyjna systemów telematyki transportu*. Prace Naukowe Politechniki Warszawskiej, seria Transport, Nr 67, Warszawa 2009.
10. Siergiejczyk M.: *Utrzymanie gotowości sieci telekomunikacyjnej z wykorzystaniem sytemu zarządzania*. Monografia Metody utrzymania gotowości systemów. Materiały XXXVI Zimowa Szkoła Niezawodności – Szczyrk 2008. Wydawnictwo Instytutu Technologii Eksploatacji, Radom 2007.
11. Sosinsky B.: *Sieci komputerowe*. Wydawnictwo Helion 2011.
12. Stawowski M. *Techniczny biuletyn zabezpieczeń IT*. Clico Sp. z o .o 2003
13. Ustawa z dnia 27 lipca 2012 r. o zmianie ustawy o drogach publicznych. Dz. U. Poz. 965. Warszawa, dnia 28 sierpnia 2012 r.
14. Wawrzyński W., Siergiejczyk M. i in.: *Metody wykorzystania środków telematyki we wspomaganiu realizacji zadań transportowych*. Grant KBN 5T12C 066 25. Warszawa 2006.

Some problems of data transmission safety in ITS

In article was presented aims and tasks of Intelligent Transport System, which are width set of difference technology and methods management , they are use in transport systems. ITS helps in safety of participants life, safety of natural environments. By adequate factors and telecommunication system efficiency of ITS is higher.

Keywords: Intelligent Transportation Systems, IT technology, safety of transmission.

Autorzy:

prof. nadzw. dr hab. inż. **Mirosław Siergiejczyk** – Politechnika Warszawska

Daria Korczak – Politechnika Warszawska