Stanisław KONATOWSKI[1], Maciej GOŁGOWSKI[2]

Wojskowa Akademia Techniczna, Wydział Elektroniki (1), 41. Baza Lotnictwa Szkolnego (2)

doi:10.15199/48.2017.10.15

Koncepcja systemu monitorowania ruchu pojazdów drogowych

Streszczenie. *Dokładne określanie położenia pojazdu drogowego jest jedną z najważniejszych kwestii w transporcie. Systemy monitorujące ruch pojazdów korzystają z osiągnięć informatyki, telekomunikacji, elektroniki i nawigacji satelitarnej. Skuteczną metodą zwiększenia bezpieczeństwa oraz przestrzegania i nieuchronnego egzekwowania prawa w ruchu drogowym mogłoby stać się wprowadzenie centralnego systemu monitorowania ruchu pojazdów, stale rejestrującego położenie i prędkość pojazdów oraz dane kierowcy. Artykuł przedstawia koncepcję systemu uwzględniającą bezpieczeństwo danych użytkownika.*

Abstract. *Precise determination of a vehicle location is one of the most significant issues in the field of transport. Movement monitoring systems for road vehicles are strictly base on achievements of telecommunications, electronics and satellite positioning systems. One of the most efficient ways to improve road safety and law enforcement in road traffic would be introduction of a global vehicle movement monitoring system, constantly supervising position and speed of vehicles along with driver personal data. The paper presents an idea of a movement monitoring system for road vehicles. (**Movement monitoring system for road vehicles**).*

Słowa kluczowe: system monitorowania położenia, telematyka, mechatronika samochodowa.
Keywords: position monitoring system, telematics, car mechatronics telematics.

Wprowadzenie

Dokładne określanie położenia pojazdu drogowego jest jedną z najważniejszych kwestii w transporcie. Satelitarne systemy pozycjonowania GNSS (*Global Navigation Satellite System*) mają szerokie zastosowanie w sektorze drogowym (transportowym), poczynając od monitorowania pozycji pojazdów, poprzez samochodowe odbiorniki nawigacyjne i automatyczne systemy obsługujące drogi płatne, kończąc na zastosowaniach związanych z bezpieczeństwem w ruchu drogowym. W transporcie drogowym systemy określania pozycji mają szczególne zastosowanie w dziedzinach takich jak [1,2,7,17]:

- monitorowanie pozycji jednostek transportowych ze specjalnym uwzględnieniem pojazdów przewożących ludzi oraz materiały niebezpieczne,
- zarządzanie i sterowanie flotami pojazdów,
- nawigacja pojedynczych obiektów transportowych,
- poprawa poziomu bezpieczeństwa w transporcie.

Dodatkowym atutem wynikającym z użycia systemów pozycjonujących pojazdy jest możliwość wykrycia faktu ich kradzieży i w następstwie tego ustalenia dokładnego miejsca ukrycia. W Polsce w dalszym ciągu dokonywane są przestępstwa kradzieży pojazdów, które giną z ulic i dróg lub parkingów samochodowych [18]. Wykrywalność tego zjawiska jest stosunkowo niska – udaje się wskazać sprawców zaledwie co czwartego przestępstwa [3].

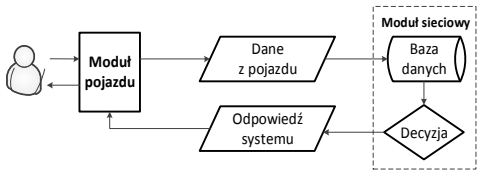
Zastosowanie systemów satelitarnych w transporcie samochodowym

Niskie ceny odbiorników satelitarnych powodują dużą dostępność systemów nawigacji samochodowej. Aktualnie w Unii Europejskiej ponad ćwierć miliarda pojazdów jest wyposażonych w nawigację satelitarną. Gwarantuje to ciągły rozwój technologii przeznaczonych dla użytkowników tego segmentu takich jak: odbiorniki satelitarne wraz z mapami cyfrowymi, systemów informowania o sytuacji na drogach i bazie turystycznej, serwisów pogodowych itp. Producenci pojazdów w dużej mierze oferują wbudowane odbiorniki nawigacyjne, aczkolwiek istnieją także bardzo popularne, uniwersalne systemy nawigacji wykorzystujące urządzenia mobilne. Spotykane rozwiązania oferują szeroki wachlarz możliwości. Oprócz standardowych dostępnych opcji określania i wizualizacji położenia pojazdu na cyfrowej mapie, dostępne są także opcje wyszukiwania i planowania trasy przejazdu, obliczania jej parametrów (czasu, odległości), planowania miejsc odpoczynku, uruchomienia systemu automatycznego przesyłania informacji *eCall* i zdalnego serwisowania pojazdu. Często poza standardowo dostarczanymi mapami, aktualizowanymi w urządzeniu okresowo, producenci oferują opcję automatycznego aktualizowania mapy oraz informacje o sytuacji na drogach poprzez komórkową transmisję danych [2].

Transport, pomimo rozwoju technologicznego jaki dokonał się w ostatnich kilkunastu latach, wciąż zalicza się do niebezpieczniejszych dziedzin gospodarki poprzez występowanie dużej liczby wypadków drogowych z ofiarami śmiertelnymi lub poważnymi uszczerbkami na zdrowiu [7,18]. Rozwijanie nawigacyjnych systemów satelitarnych oraz powszechnego dostępu do nich może wpłynąć na poprawę bezpieczeństwa w Polsce i zmniejszenie liczby wypadków w porównaniu do innych krajów europejskich. Popularyzacja nawigacji satelitarnej i systemów z nią związanych doprowadzi także do zwiększenia niezawodności i efektywności transportu, a w efekcie do oszczędności [2,7].

System monitorowania ruchu pojazdów drogowych

Najbardziej skuteczną metodą zwiększenia bezpieczeństwa oraz przestrzegania i nieuchronnego egzekwowania prawa w ruchu drogowym byłoby wprowadzenie systemu monitorowania ruchu pojazdów drogowych (SMRP), czyli ciągłego rejestrowania położenia i prędkości pojazdów oraz danych kierowcy. W początkowej fazie system mógłby testowo obejmować tylko kierowców i pojazdy transportu miejskiego. Dałoby to możliwość dodatkowego wykorzystania systemu do obsługi pasażerów – możliwość wybrania najbliższej wolnej taksówki czy sprawdzenie pozycji autobusu. System ten zapewniałby także nadzorowanie zachowania kierowcy zwiększając bezpieczeństwo przewożonych pasażerów lub ładunków.



Rys. 1. Idea działania systemu monitorowania ruchu pojazdów

Proponowany system składa się z modułu sieciowego – Centralnej Bazy Danych (CBD) współdziałającej z systemami zewnętrznymi oraz z modułu pojazdu (MP),

który współpracuje z kamerami, odbiornikiem GPS (*Global Positioning System*) i modułem GSM (*Global System for Mobile Communications*), a także z czytnikiem kart elektronicznego prawa jazdy (EPJ) [7,17].

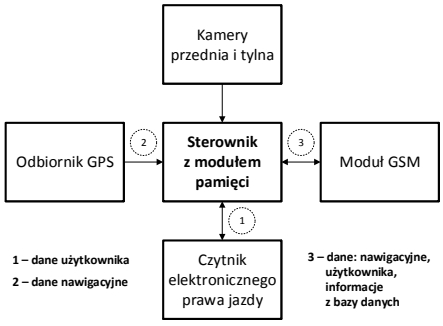
Schemat działania systemu pokazuje rysunek 1. W pojeździe zainstalowany jest moduł sterujący gromadzący dane z urządzeń peryferyjnych (kamery, odbiornik GPS) i przekazujący je wraz z danymi kierowcy do Centralnej Bazy Danych w celu zapisania, weryfikacji oraz kontroli. Końcowe wyniki, np. liczba punktów karnych kierowcy, są przekazywane do modułu pojazdu, który informuje kierowcę o otrzymanych powiadomieniach. Ponadto moduł sieciowy może informować odpowiednie służby (systemy) o próbie kradzieży pojazdu lub jego nieuprawnionym użyciu itp.

Moduł sieciowy

Centralna Baza Danych jest głównym elementem systemu. Zawiera informację o kierowcy, użytkowanym przez niego pojeździe i pozycji (trasie). Umożliwia ona przetwarzanie danych na potrzeby służb porządkowych i informowanie patroli o zagrożeniach w ruchu drogowym. Całość komunikacji odbywa się w oparciu o istniejącą infrastrukturę sieci GSM. Dane wrażliwe są zaszyfrowane i zabezpieczone.

Moduł pojazdu

Moduł pojazdu składa się z kamer, odbiornika GPS, modułu GSM i czytnika prawa jazdy. Użytkownik w pierwszej kolejności wczytuje przykładając do urządzenia kartę prawa jazdy w standardzie MIFARE [4,8,9]. Zapisane są w niej dane kierowcy (w postaci zaszyfrowanej), które będą weryfikowane w CBD. Kamery nagrywają obraz w trybie ciągłym zapisując go w pamięci urządzenia. Moduł pojazdu, poprzez swój sterownik, mógłby analizować obraz odczytując znaki drogowe i ustalając dopuszczalną prędkość pojazdu. Po ustaleniu pozycji i prędkości przesyłałby do CBD także informacje o popełnionych wykroczeniach.



Rys. 2. Schemat modułu pojazdu

Podczas projektowania systemu monitorowania ruchu pojazdów uwzględniono bezpieczną identyfikację i uwierzytelnianie użytkownika za pomocą karty elektronicznej. W systemie zastosowana zostanie szyfrowana transmisja danych między modułem pojazdu, a bazą CBD z wykorzystaniem transmisji SSL (*Secure Socket Layer*) zwiększającej bezpieczeństwo danych [1,2,16]

Elementy Modułu Pojazdu

Głównym elementem przykładowego modułu nawigacyjnego pojazdu może być mikrokontroler z rodziny STM32f3 z rdzeniem Cortex M4. Mikrokontroler taktowany jest zegarem o częstotliwości 72 MHz, posiada 48 kB pamięci RAM oraz 256 kB pamięci Flash. Dodatkowo może współpracować z żyroskopem np. L3GD20 w celu monitorowania przechyleń pojazdu w czasie postoju (wykorzystanie pośrednio do detekcji kradzieży). Żyroskop służy do pomiaru prędkości kątowej w trzech osiach o maksymalnym zakresie pomiarowym do 2000 deg/s. Przesyłanie danych o prędkości kątowej do mikrokontrolera w tym przykładzie odbywałoby się poprzez interfejs SPI (*Serial Peripheral Interface*). Mikrokontroler jako element główny MP odpowiedzialny jest za komunikację ze wszystkimi modułami urządzenia oraz odpowiednie przetwarzanie danych. W propozycji Modułu Pojazdu systemu monitorowania wymagane będą dwa porty szeregowe USART (*Universal Synchronous and Asynchronous Receiver and Transmitter*) oraz interfejs SPI w przypadku użycia ww. żyroskopu. USART wykorzystuje tylko dwie linie danych – linię TX (transmisji) oraz RX (odbioru). Do określania pozycji pojazdu służy odbiornik GPS, wykorzystujący na przykład układ FGPMMOPA6H [5], pracujący w standardzie NMEA [7]. Zarówno mikrokontroler jak i odbiornik umożliwiają prostą i wystarczająco szybką transmisję między sobą, wykorzystując interfejs USART. Dane z odbiornika GPS przesyłane są do procesora w postaci kodów ASCII. Każda ramka danych rozpoczyna się znakiem “$”, po którym występuje identyfikator typu danych, dane, suma kontrolna, a po niej znak powrotu karetki <CR> i nowej linii <LF>. W szeregu przesyłanych ramek najbardziej interesujące, w aspekcie określania położenia, są ramki GPRMC oraz GPGGA. Dane nawigacyjne, po odpowiednim przetworzeniu w mikrokontrolerze, przesyłane są do modułu GSM na przykład Fibocom G510 [6]. Transfer danych odbywa się także poprzez interfejs USART z wykorzystaniem komend AT. Umożliwia to bezproblemową komunikację z dowolnym modułem GSM/telefonem, niekoniecznie wymienionym wcześniej. Jednakże wymaga to zainstalowania karty SIM z aktywną usługą transmisji w sieci GPRS (*General Packet Radio Service*) [7]. Możliwość obsługi przez proponowany mikrokontroler wielu interfejsów dla urządzeń peryferyjnych, pozwala na rozbudowę MP o dodatkowe elementy takie jak moduł Bluetooth do komunikacji ze smartfonem kierowcy, czujniki zbliżeniowe czy podczerwieni.

Elektroniczne prawo jazdy / token identyfikacyjny

Do odczytu danych z transpondera (karty) wykorzystuje się czytnik będący urządzeniem nadawczo-odbiorczym wraz z anteną. Karta elektroniczna lub token wykorzystuje fale radiowe do transmisji danych oraz jej zasilania. Czytnik wytwarza pole elektromagnetyczne (dla MIFARE o częstotliwości 13,56 MHz). Karta, posiadająca układy rezonansowe dostrojone do tej częstotliwości, gromadzi energię fali w kondensatorach i gdy osiągnie ona odpowiednią wartość, układ scalony karty emituje zakodowany sygnał odpowiedzi. Może zawierać on unikalny numer karty oraz dodatkowe dane zapisane na karcie. Urządzenie nie posiada własnego źródła zasilania, dlatego do pracy wymaga zbliżenia do czytnika na odległość do 10 cm. Karta w standardzie MIFARE Plus posiada także zaimplementowany algorytm szyfrujący AES-128, który zapewnia wyższy poziom bezpieczeństwa w porównaniu do standardu MIFARE Classic używającego tylko autorskiego algorytmu Crypto1. Algorytm szyfrujący wymaga jednak aby czytnik posiadał odpowiadający karcie klucz. W tym celu po nawiązaniu bezpiecznego połączenia MP przesyła do CBD UID (unikalny numer identyfikacyjny EPJ) i otrzymuje z bazy odpowiadający mu 128 bitowy klucz K_k, który zostanie wykorzystany do uwierzytelnienia karty, odczytania i aktualizacji danych. Karta posiada 4 kB pamięci EEPROM w 32 sektorach po 4 bloki i 8 sektorów po 16 bloków, w których można przechowywać dowolne dane [4,8]. W przypadku SMRP będą to dane kierowcy, punkty karne, uprawnienia do prowadzenia pojazdów, alerty (np. osoba

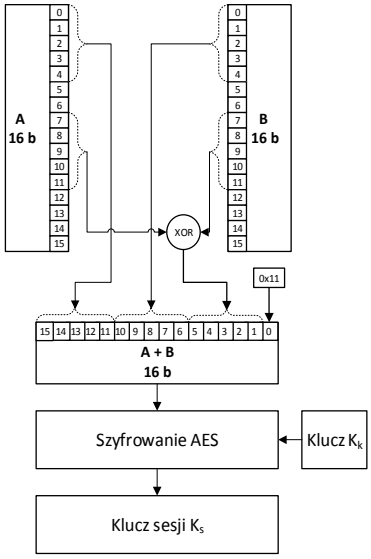
poszukiwana, odebranie uprawnień). Kontrola mogłaby odbywać się przy założeniu, że każda karta będzie posiadała taki sam klucz nadrzędny Master Key dostępny tylko dla urządzeń kontrolnych. Pozwoli to na odczytanie danych z karty bez konieczności połączenia z CBD.

Rys. 3. Token i karty w standardzie MIFARE [8]

Uwierzytelnianie EPJ

EPJ jako karta w standardzie MIFARE Plus pozwala na uwierzytelnienie jej w czytniku (w trybie zabezpieczeń karty poziomu trzeciego) przy użyciu szyfrowania algorytmem AES. Cały proces uwierzytelniania jak i następująca po nim wymiana danych jest także zaszyfrowana tym samym algorytmem, ale z innym kluczem. Dzięki temu minimalizowane jest ryzyko wycieku danych osobowych z karty [9,10,13]. Proces ten wymaga posiadania przez czytnik klucza K_k przypisanego do karty. W SMRP jest on pobierany z serwera CBD w następującej kolejności [11]:

1. MP (czytnik) przesyła komendę uwierzytelnienia EPJ (karty) wraz z numerem klucza.
2. EPJ odczytuje z pamięci wybrany klucz K_k, generuje 16 bitową liczbę pseudolosową B i szyfruje ją kluczem K_k. Następnie wysyła ją do MP.
3. MP odszyfrowuje liczbę B kluczem K_k otrzymując wygenerowaną przez EPJ liczbę B, generuje pseudolosową 16 bitową liczbę A, przesuwa liczbę B w lewo o 8 bitów tworząc liczbę B', scala liczby B' oraz A (rezultatem jest 32 bitowa liczba), szyfruje je kluczem K_k i przesyła do MP.

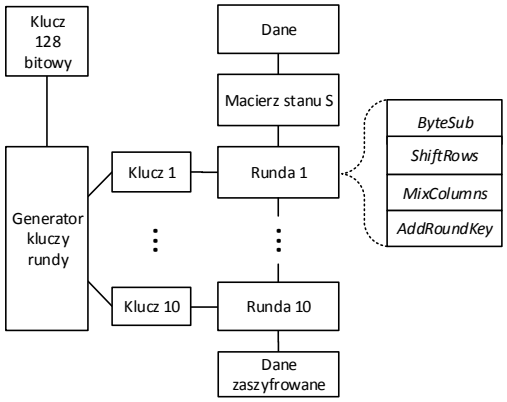


Rys. 4. Generacja klucza sesji

4. EPJ po odebraniu danych deszyfruje je kluczem K_k , rozdziela otrzymaną liczbę na A i B', porównuje B' z liczbą B wygenerowaną uprzednio i przesuniętą w lewo o 8 bitów. Jeżeli są zgodne oznacza to, że dane są poprawne i karta posiada właściwą liczbę A. EPJ przesuwa w lewo liczbę A o 8 bitów tworząc liczbę A' którą szyfruje kluczem K_k i przesyła do MP.
5. MP po otrzymaniu danych deszyfruje je kluczem K_k, porównuje liczbę A przesuniętą o 8 bitów w lewo z odebraną liczbą A' i jeżeli są równe uwierzytelnia EPJ generując klucz sesji K_s – zgodnie z rys. 4.

Szyfr blokowy

Szyfr blokowy AES (*Advanced Encryption Standard*) jest szyfrem z tajnym symetrycznym kluczem (szyfrującym i jednocześnie deszyfrującym). W systemie SMRP wykorzystuje 128 bitowy klucz szyfrując dane w postaci również 128 bitowych bloków (reprezentowanych w algorytmie jako macierz stanu o wymiarze 4 x 4 bajty) [12]. Charakteryzuje się on dużą szybkością działania i niskim użyciem pamięci przez co efektywnie funkcjonuje w wielu urządzeniach, np. w kartach elektronicznych. Rozmiar klucza definiuje liczbę transformacji w algorytmie szyfrującym, w tym przypadku jest to dziesięć rund szyfrujących. W ich skład wchodzą: *AddRoundKey* – dodanie klucza rundy do szyfrowanych danych, *MixColumns* – przekształcenie kolumny macierzy stanu, *ShiftRows* – przesunięcie cykliczne wierszy macierzy stanu, *SubBytes* – zamiana bajtów macierzy stanu. Jako pierwsza transformacja wykonywana jest *AddRoundKey*, a następnie kolejno rundy algorytmu w kolejności: *SubBytes*, *ShiftRows*, *MixColumns*, *AddRoundKey* (w ostatniej rundzie algorytmu nie jest wykonywana *MixColumns*).



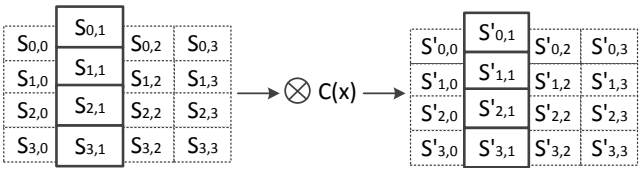
Rys. 5. Schemat ogólny algorytmu AES

Transformacja *AddRoundKey* polega na dodaniu kolejnych bajtów klucza rundy do bajtów macierzy stanu przy pomocy operacji bitowej XOR.

$$\begin{bmatrix} S_{0,0} & S_{0,1} & S_{0,2} & S_{0,3} \\ S_{1,0} & S_{1,1} & S_{1,2} & S_{1,3} \\ S_{2,0} & S_{2,1} & S_{2,2} & S_{2,3} \\ S_{3,0} & S_{3,1} & S_{3,2} & S_{3,3} \end{bmatrix} \oplus \begin{bmatrix} K_{0,0} & K_{0,1} & K_{0,2} & K_{0,3} \\ K_{1,0} & K_{1,1} & K_{1,2} & K_{1,3} \\ K_{2,0} & K_{2,1} & K_{2,2} & K_{2,3} \\ K_{3,0} & K_{3,1} & K_{3,2} & K_{3,3} \end{bmatrix} = \begin{bmatrix} S'_{0,0} & S'_{0,1} & S'_{0,2} & S'_{0,3} \\ S'_{1,0} & S'_{1,1} & S'_{1,2} & S'_{1,3} \\ S'_{2,0} & S'_{2,1} & S'_{2,2} & S'_{2,3} \\ S'_{3,0} & S'_{3,1} & S'_{3,2} & S'_{3,3} \end{bmatrix}$$

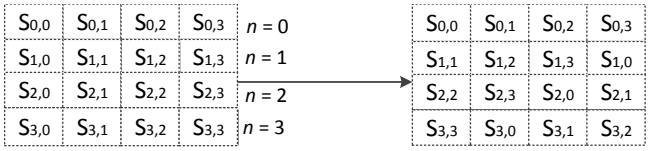
Rys. 6. Transformacja *AddRoundKey*

Transformacja *MixColumns* działa na kolumnach macierzy stanu (słowach), które są interpretowane jako wielomian S(x) i są mnożone przez stały wielomian C(x). Wynikiem tych działań jest wielomian S'(x), którego współczynniki są elementami macierzy stanu S'.



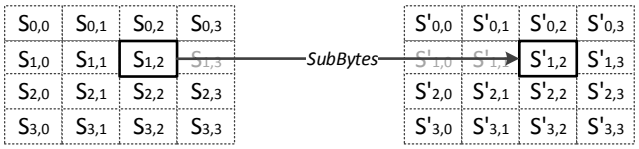
Rys. 7. Transformacja *MixColumns*

Transformacja *ShiftRows* przesuwa element macierzy w lewo o „*n*" pozycji bajtowych, gdzie liczba „*n*" jest równa numerowi wiersza w macierzy stanu.



Rys. 8. Transformacja *ShiftRows*

Transformacja *SubBytes* wykonuje podstawienia w macierzy stanu na wartości bajtowe z tablicy podstawień. Wprowadza to większą nieliniowość przekształceń podczas szyfrowania.

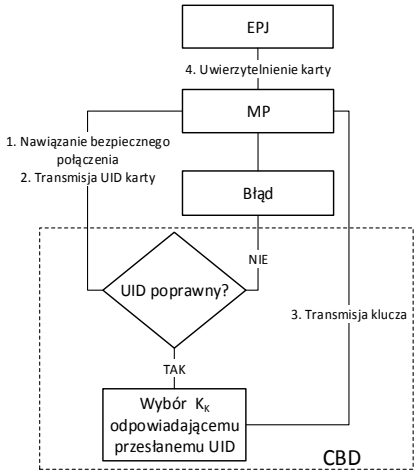


Rys. 9. Transformacja *SubBytes*

W proponowanym algorytmie szyfrującym klucz można w obecnym czasie złamać jedynie poprzez atak typu „*brute force*”. Polega on na sprawdzaniu wszystkich kombinacji klucza, co przy zastosowaniu 128 bitowego szyfrowania zapewnia 2^{128} możliwych kombinacji. Czas potrzebny do wykonania tego zadania zależy od czasu wykonania pojedynczego sprawdzenia T oraz długości klucza *N* [10]. W najgorszym przypadku jest to 2^{128}*T, a w optymalnym przypadku klucz zostanie złamany po połowie możliwych prób, czyli po czasie równym 2^{127}*T. Zakładając użycie superkomputera, dla którego T wyniosłoby 10^{-10} s, czas potrzebny do złamania klucza metodą „*brute force*” wynosi w przybliżeniu $5{,}4*10^{20}$ lat. Istnieją także metody ataku na ten rodzaj szyfrowania, które polegają na analizie przebiegu algorytmu szyfrującego i modyfikacji jego parametrów poprzez oddziaływanie na urządzenie realizujące proces szyfrowania, tak zwane „*side-channel attacks*” [13]. Odporność na tego typu inwazyjne ataki musi zapewnić fizyczna konstrukcja urządzenia (MP).

Transmisja danych

Transmisja danych pomiędzy sterownikiem w pojeździe, a bazą danych odbywa się poprzez sieć GSM – protokół TCP zabezpieczony przez standard SSL (*Secure Socket Layer*), umożliwiający bezpieczną transmisję przy użyciu certyfikatów.



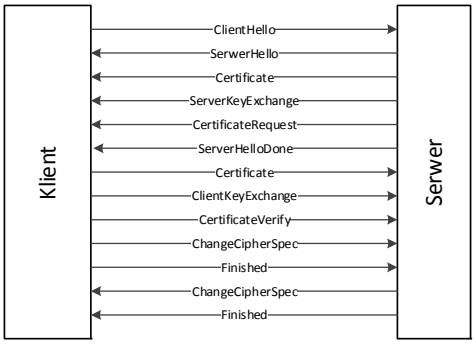
Rys. 10. Schemat przepływu danych

Należy umieścić token (w standardzie MIFARE jedną kartę) w polu czytnika co umożliwi przesyłanie zapytanie o UID. Po jego odebraniu czytnik nawiązuje bezpieczne połączenie z CBD poprzez protokół SSL i przesyła tak zabezpieczony UID karty. Jako informację zwrotną czytnik otrzymuje klucz uwierzytelniający karty K_K. Jest on wymagany do odczytania pozostałych danych z EPJ. Jako iż połączenie internetowe i transmisja danych jest wymagana do użycia EPJ, w obszarach poza zasięgiem sieci GSM projektowany system nie będzie funkcjonować. W przypadku terenu Polski, obszar ten jest minimalny [14].

Protokół transmisji szyfrowanej SSL

SSL jest protokołem typu klient-serwer umożliwiającym bezpieczne połączenie szyfrowane. Protokół pozwala na uwierzytelnienie serwera jak również klienta. Według modelu OSI (pełna nazwa *Open Systems Interconnection Reference Model*) działa on w warstwie prezentacji [15], co pozwala zabezpieczać protokoły warstwy najwyższej.
Sesja SSL przebiega następująco [16]:

1. nawiązanie połączenia wykorzystując protokół TCP (*Transmission Control Protocol*),
2. wymiana danych (obsługiwanie, algorytmy szyfrowania, certyfikaty),
3. uzgodnienie wspólnego zbioru algorytmów,
4. potwierdzenie tożsamości serwera i klienta,
5. wymiana kluczy sesyjnych,
6. transmisja danych.



Rys. 11. Schemat sesji SSL

Schemat uwierzytelnienia klienta (MP) jak i serwera (CBD) przedstawia rys. 11. Zwrot strzałek określa kierunek transmisji w protokole.

- *ClientHello* – przesyłane jest do serwera zapytanie zawierające informację o obsługiwanym protokole, algorytmach szyfrujących i algorytmach kompresujących dane, identyfikatorze sesji oraz liczbie pseudolosowej wykorzystywanej do generowania kluczy.
- *ServerHello* – odpowiedź serwera kryjąca parametry połączenia, wersję protokołu, parametry szyfrowania, kompresji oraz liczbę pseudolosową.
- *Certificate* – serwer przesyła swój certyfikat.
- *ServerKeyExchange* – serwer przesyła swój klucz publiczny.
- *CertificateRequest* – transmitowane jest zapytanie do klienta o jego własny certyfikat.
- *ServerHelloDone* – komunikat przesyłany o gotowości serwera do dalszego zestawiania połączenia.
- *Certificate* – klient odsyła do serwera swój certyfikat.
- *ClientKeyExchange* – transmitowany jest klucz sesji, który jest zabezpieczony publicznym kluczem serwera wygenerowanym przy użyciu liczb pseudolosowych.
- *CertificateVerify* – sprawdzana jest poprawność certyfikatu klienta poprzez podpisanie kluczem prywatnym wszystkich dotychczas ustalonych parametrów połączenia i przesłanie ich do serwera.
- *ChangeCipherSpec* – przesyłane są komunikaty o przejściu do transmisji danych szyfrowanych.

– *Finished* – transmitowane są dane zawierające zaszyfrowany MAC (kod uwierzytelnienia wiadomości), który odbiorca deszyfruje i sprawdza jego integralność. Jeżeli MAC nie jest zgodny to połączenie jest błędnie uwierzytelnione i dalsza transmisja nie następuje.

Możliwe jest odtworzenie przerwanego lub zakończonego połączenia SSL bez ponownego uwierzytelnienia obu stron. W komunikacie *ClientHello* zawarty jest numer identyfikacyjny ostatniej sesji, jeżeli serwer go rozpozna to wymiana danych może być zabezpieczona poprzednio wygenerowanym kluczem.

Centralna Baza Danych

Relacyjna baza CBD zawiera dane użytkowników wprowadzone przez administratora systemu. Numer UID Elektronicznego Prawa Jazdy jest przyporządkowany w bazie do użytkownika, umożliwiając dostęp jedynie przy jego użyciu. Ponadto baza zawiera klucz, który służy do identyfikacji i uwierzytelnienia między MP a EPJ.

Tab. 1. Struktura danych w CBD dla pojedynczego użytkownika

Baza użytkownika				
Tabela 1			**Tabela 2**	
UID	Dane identyfikacyjne	Klucz EPJ	Dane nawigacyjne	Alerty
7 bajtów	Pozostałe informacje	128 bitów	Prędkość	Wyróżnione dane
	Uprawnienia do kierowania pojazdami		Pozycja	
	PESEL		Czas	
	Imię i nazwisko		Data, godzina, pozycja pojazdu, prędkość	

Gdy CBD prześle klucz karty do MP, zapisuje UID w tabeli MP. Tabela MP zawiera dane o użyciu czytników (pojazdów) przez użytkowników. Zapisywane w niej są także dane o zaprzestaniu użycia pojazdu. Umożliwia to identyfikację kierowcy w danym okresie użytkowania oraz analizę wykorzystania EPJ. W polu Dane dodatkowe mogą być umieszczone informacje wygenerowane przez MP, a dotyczące błędów urządzenia lub połączenia.

Tab. 2. Struktura danych w CBD dla pojedynczego modułu pojazdu

Tabela MP			
UID	Wymagane uprawnienia	Data i czas rozpoczęcia, zakończenia	Dane dodatkowe (brak połączenia, uprawnień)

Częstotliwość dodawania rekordów do bazy uzależniona jest od priorytetu użytkownika, który może być definiowany przez MP lub samą CBD. Pozwala to na pierwszeństwo pojazdów użytku publicznego lub użytkowników zwiększonego ryzyka nad innymi. Dane te są zapisane w pamięci EPJ i mogą być modyfikowane przez algorytmy CBD przy użyciu czytnika MP.

Podsumowanie

Przedstawiony projekt SMRP pozwoli na zarządzanie i nadzorowanie ruchem pojazdów. Jego ważną cechą jest bezpieczeństwo danych użytkownika, które musi być zapewnione na każdym etapie jego użytkowania. Zapobiega to upływowi danych osobowych do osób niepowołanych. Proponowane metody i algorytmy transmisji jak i autoryzacji klienta uchodzą za bezpieczne i odporne na większość ataków. Zakładając prawidłową konstrukcję MP jak i jego zabezpieczenie można wnioskować, że system ten spełni zakładane założenia użytkowe – zapewniając jednocześnie bezpieczeństwo danych. Jednakże z każdym rokiem zwiększa się moc obliczeniowa komputerów, co skutkuje zwiększeniem prawdopodobieństwa znalezienia słabości algorytmu szyfrującego czy też zmniejszeniem czasu potrzebnego do jego złamania. Dlatego też w przypadku wdrożenia rozwiązania, wszystkie zabezpieczenia muszą być aktualizowane zgodnie z najnowszymi trendami bezpieczeństwa. Kosz obsługi prezentowanego systemu zależy w dużej mierze od jego powszechności. Zwiększenie liczby użytkowników systemu spowoduje spadek kosztu jednostkowego. Opłatą instalacji urządzenia w pojeździe można obciążać producenta pojazdu lub jego użytkownika. Operator poniesie wydatki związane tylko z transmisją danych z CBD.

***Autorzy**: dr inż. Stanisław Konatowski, Wojskowa Akademia Techniczna, Wydział Elektroniki, ul. gen. Sylwestra Kaliskiego 2, 00-908 Warszawa, E-mail: skonatowski@wat.edu.pl, mgr inż. Maciej Gołgowski, 41. Baza Lotnictwa Szkolnego, E-mail: mgolgowski@gmail.com*

LITERATURA

[1] Templin T., Tyszko A., Oszczak B: *Monitoring ruchu na drogach*, Polskie Biuro ds. Przestrzeni Kosmicznej.
[2] Maciejewski M., Waleriańczyk W., Janiak P.: *Porównanie systemów monitorowania i nawigacji dla floty pojazdów dostępnych na polskim rynku*, Logistyka, 2/2010, str. 1833-1842.
[3] http://statystyka.policja.pl/st/wybrane-statystyki/kradzieze-samochodow.
[4] Nota katalogowa MIFARE Plus - MF1SPLUSx0y1 NPX 2016.
[5] Nota katalogowa układu FGPMMOPA6H.
[6] Nota katalogowa układu FIBOCOM G510.
[7] Konatowski S., Gołgowski M.: *System monitorowania położenia pojazdów floty*, Przegląd Elektrotechniczny, R. 91, Nr 10/2015, str. 211-215.
[8] https://www.nfc24.pl/clamshell-mifare-nfc.
[9] Bienert R.: *MIFARE Plus technical details*, NPX 2011.
[10] Norma ISO/IEC 14443: *Identification cards - Contactless integrated circuit(s) cards - Proximity cards*, część 1-4.
[11] Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, 2001.
[12] Karbowski M.: *Podstawy Kryptografii*, Helion 2014.
[13] Hancke G.: *A Practical Relay Attack on ISO 14443 Proximity Cards*, University of Cambridge.
[14] Urząd Komunikacji Elektronicznej: *Raport z badania porównawczego wartości wskaźników jakości usług w sieciach ruchomych przedsiębiorców telekomunikacyjnych w Polsce*, 2015 r.
[15] Comer D.E., *Sieci komputerowe TCP/IP - zasady, protokoły i architektura*, WNT, 1998.
[16] Diersk T., Rescorla E.: *The Transport Layer Security (TLS) Protocol*, 2008.
[17] Chen F., Jia Y., Li J.: *Research of Integrated Control Methods and its Simulation for Freeway Mainline and Related Ramp*, Przegląd Elektrotechniczny, R. 88, Nr 1b/2012, str. 119-122.
[18] Kukiełka J.: *Prognozowanie ruchu na drogach krajowych*, Budownictwo i Architektura, Nr 10/2012, str. 131-144.