Studia i Materiały Informatyki Stosowanej, Tom 6, Nr 16, 2014
str. 16-20

SYSTEM ŁĄCZNOŚCI DO MONITOROWANIA WYPOSAŻENIA I JEDNOSTEK STRAŻY POŻARNEJ

Tomasz Z. Kosowski, Marek Jeliński, Paweł Stosik, Rafał Motylewski

TELDAT
ul.Cicha 19-27, 85-650 Bydgoszcz
e-mail: {tkosowski, mjelinski, pstosik, rmotylewski}@teldat.com.pl

Streszczenie: *Skuteczny i pewny system łączności jest warunkiem poprawnej pracy każdego systemu monitorowania. Systemy specjalnego przeznaczenie jak np. systemy używane przez Straż Pożarną muszą pracować we wszystkich warunkach środowiskowych. Budowa systemu monitorowania wymaga opracowania czujników i systemu komunikacji. Sensory powinny dostarczać informacji o stanie urządzenia. Informacja z sensorów powinna być przekazywana do stacji monitorowania w sposób szybki i pewny. Niniejszy artykuł przedstawia możliwości budowy systemu łączności dla monitorowania urządzeń i jednostek straży pożarnej. W artykule przedstawiono wyniki pomiarów wybranych środków łączności oraz możliwości zastosowania odpowiednich protokołów transmisji.*

Słowa kluczowe: *CDMA, transmisja danych, 802.11*

Transmission system for monitoring equipment and fire brigade units

Abstarct: *Efficient and reliable communications system is a prerequisite for the correct operation of each monitoring system. Special systems like used by fire brigade must work well in all conditions. Therefore some special sensors and communications system must be designed. These sensors have to provide information about equipment condition. Information from sensors have to be passed in quick and reliable way. This article presents the possibility of building a communications system for monitoring equipment and fire brigades. Communication equipments and protocols are described. The article presents the results of tests of selected means of communication and the possibility of the use of appropriate protocols.*

Keywords: *CDMA, data transmission, 802.11*

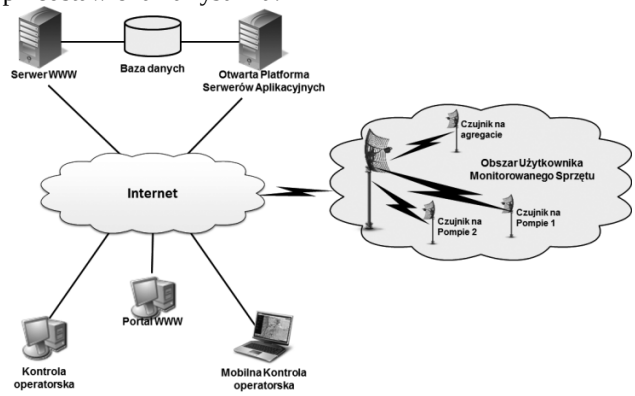
1. WSTĘP

W ramach czwartego konkursu NCBiR na rzecz obronności i bezpieczeństwa państwa realizowany jest projekt rozwojowy numer DOBR-BIO4/051/13087/2013, „Opracowanie metodologii stałego nadzoru eksploatacji wybranych obszarów wyposażenia straży pożarnej w zakresie niezawodności i skuteczności działania". Celem projektu jest opracowanie zaawansowanych technologii informatycznych wspomagających zarządzanie kryzysowe i ratownictwo, stworzenie demonstratora technologii – systemu teleinformatycznego zbierającego i przetwarzającego dane oraz wspierającego zadania logistyczne w zakresie serwisowania oraz zakupów sprzętu ratowniczego, a także zawierającego bazę świadectw dopuszczeń wydawanych przez CNBOP – PIB.

Demonstrator technologii systemu zostanie zainstalowany i sprawdzony w warunkach operacyjnych. Będzie to system informatyczny zbierający i przetwarzający dane oraz wspierający zadania logistyczne w zakresie serwisowania oraz zakupu sprzętu ratowniczego, a także zawierający bazę świadectw dopuszczenia wydawanych przez CNBOP.

W skład systemu wejdzie serwer aplikacji, stanowiący jego punkt centralny, modularna aplikacja kliencka pozwalająca na dostęp do systemu oraz interfejs WWW pozwalający na dostęp do systemu przy pomocy przeglądarki internetowej. Konsole operatorskie: cztery stacjonarne, znajdujące się w centrum dowodzenia oraz dwie zdalne umożliwiające podczas akcji, na bieżąco, monitoring floty biorącej w niej

udział. Planowana architektura systemu została przedstawiona na rysunku.



Rysunek. 1 Architektura systemu [1].

Końcowym produktem projektu będzie demonstrator systemu diagnostyki technicznej wyposażenia straży pożarnej. Na elementy demonstratora będą się składały:

- system sensorów monitorujący stan wybranych urządzeń;
- system łączności pozwalający na przesyłanie na bieżąco w warunkach operacyjnych danych pozyskanych z sensorów do systemu informatycznego oraz pozwalający na zdalny dostęp do stworzonego systemu;
- system informatyczny zbierający i przetwarzający dane oraz wspierający zadania logistyczne w zakresie serwisowania oraz zakupu sprzętu ratowniczego.

2. IDENTYFIKACJA I TESTY ŚRODKÓW ŁĄCZNOŚCI

Wymagania na środki łączności

Budowany demonstrator technologii musi spełniać warunki docelowej pracy systemu, mianowicie:

- posiadać system łączności pozwalający na przesyłanie na bieżąco w warunkach operacyjnych danych pozyskanych z sensorów do systemu informatycznego oraz pozwalający na zdalny dostęp do stworzonego systemu,
- zapewniać mobilność monitorowanych stacji,
- zapewniać możliwości transmisji danych z wysoką jakością transmisji i niską stopą błędów,
- zapewniać dostęp zdalny do urządzeń - możliwości dostępu zdalnego do poszczególnych urządzeń budowanego systemu celem zbierania danych, rekonfiguracji, monitorowania działania,
- gwarantować niezawodność połączeń - stabilność łączy, pewność działania,
- zapewniać stałą prędkość transmisji - możliwości szybkiej transmisji danych z uwzględnieniem wielkości danych koniecznych do przesyłania,
- gwarantować niezbędne zasięgi komunikacji pomiędzy jednostkami,
- transmisja danych z wykorzystaniem protokołu IP.

Testy środków łączności

Wybrane środki łączności muszą gwarantować osiągnięcie wymaganych parametrów do pracy systemu. Dlatego ich identyfikacja musi przebiegać pod kątem spełniania parametrów. W ramach prac zbadano i wybrano możliwe do zastosowania środki łączności.

Pierwszym z badanych środków łączności była łączność IEEE 802.11 potocznie zwana Wi-Fi.

Rysunek. 2 Mapa zasięgu łączności 802.11g, źródło: TELDAT - opracowanie własne.

Celem testu było sprawdzenie zasięgu modułów stacji klienckich - laptopów. Warunki testu były następujące:

- Access point pochodził z Systemu JAŚMIN firmy TELDAT,
- pomiar zasięgu polegał na sprawdzanie szybkości odpowiedzi na pakiety ICMP echo request do Access pointa oraz obserwacji zasięgu podawanego w statusie połączenia sieciowego w systemie Windows w skali od 0 do 5,
- w trakcie przemieszczania z punktu 1 do 2 urządzenie testowane było zwrócone przeciwnie do Access pointa, w pozostałych przypadkach – w kierunku Access pointa,
- komunikacja WiFi odbywała się zawsze na kanale 13 pasma (wcześniejsze testy pokazały, że zasięg i charakter transmisji na tym kanale jest taki sam jak na pozostałych),

- wysokość Access point i testowanego urządzenia ponad ziemią wynosiła 1 metr.

Wyniki testów:

- uzyskano stały charakter odpowiedzi na pakiety ICMP echo request w trakcie oddalania z punktu 1 do 2 – kilka milisekund, brak przekraczania limitu czasu oczekiwania na odpowiedź,
- postój wynoszący 5 minut w punkcie 2 pokazał stałe połączenie o tym samym charakterze,
- status połączenia w punkcie 2 pokazywał wartość 5 (najwyższą w skali, czyli prędkość transmisji 24Mb/s – wartość teoretyczna dla standardu pracy).

Ponadto wykonano testy stabilności połączenia Wi-Fi za pomocą urządzenia PDA z kartą USB - ETH AirLive EtherWe-1000U. Zakres testów obejmował ciągłą komunikację z urządzeniem z użyciem protokołu ICMP za pomocą polecenia ping.
Podczas całodziennych testów uzyskano następujące wyniki testu:

- maksymalna ilość momentów niedostępności urządzenia na godzinę: 11,
- minimalna ilość momentów niedostępności urządzenia na godzinę: 2,
- średnia ilość momentów niedostępności urządzenia na godzinę: 4.

Podczas testów zauważono, że momenty niedostępności urządzenia były krótkotrwałe i nie trwały dłużej niż 5-10 sekund.

Testy przywracania komunikacji po wyjęciu karty sieciowej na USB wykazały, że łączność po ponownym włożeniu karty była przywracana po ok. 15 sekundach.
Badaniom został poddany również WLAN zbudowany z wykorzystaniem anteny dookolnej firmy LUXUL wraz ze wzmacniaczem mocy, komplet jest oznaczony przez producenta jako: „HIGH PERFORMANCE TACTICAL MESH ANTENA (HP-TMA) – TMA-24A-302CT”. Najważniejsze cechy urządzeń:

- częstotliwość pracy 2400 ÷ 2500 [MHz],
- zakres temperatury pracy -40 ÷ 70 [°C],
- polaryzacja anteny dookolna,
- VSWR <2.0 : 1,
- impedancja 50 [Ω],
- EIRP chwilowe (Equivalent isotropically radiated power) 33[dBm],
- EIRP praca ciągła 27 [dBm],
- zysk anteny 2[dBi],
- czułość odbioru 17 [dB],
- akceptowalny poziom sygnału wejściowego +8 ÷ +20 [dBm],
- zasilanie podczas odbioru 2[W],
- zasilanie podczas nadawania 8[W],
- antena nie wymaga płaszczyzny uziemiającej.

Podczas testów zauważono, iż nie udało się nawiązać połączenia z prędkością większą niż 24 Mbit/s.
W wyniku testów zauważono, że urządzenia potrafią nawiązać łączność na dystansach:

- teren otwarty - 1100m,
- teren zalesiony - 280m,
- teren miejski ≈ 50m.

Tabela 1. Testy zasięgów WLAN [13]

Parametry połączenia	WLANV1 – WLANV1	WLANV2 (*bez wzmacniacza*) – WLANV2 (*ze wzmacniaczem*)	WLANV2 (*ze wzmacniaczem*) - WLANV2 (*ze wzmacniaczem*)
	Odległość	Odległość	Odległość
5,5Mb/sek., Max Pwr	~900m	-	~850m
24Mb/sek., Max Pwr	~900m	-	~850m
Best Range/Default Max Pwr	~900m	~320m	~890m

Kolejnym badanym środkiem łączności były modemy CDMA firmy AnyDATA typ ADU-500A. Zakres testów obejmował: pomiar przepływności i możliwość wykorzystania w systemie. Testowane modemy pracowały w sieci Orange.
Warunki przeprowadzanych testów:
Modemy (2 sztuki) były podłączone do dwóch komputerów pracujących z systemem Windows Xp Professional. Testy wykonywane były w godzinach 13-14, w sieci Orange z wykorzystaniem anten zewnętrznych i wewnętrznych.

Rezultaty przeprowadzonych testów przepływności:

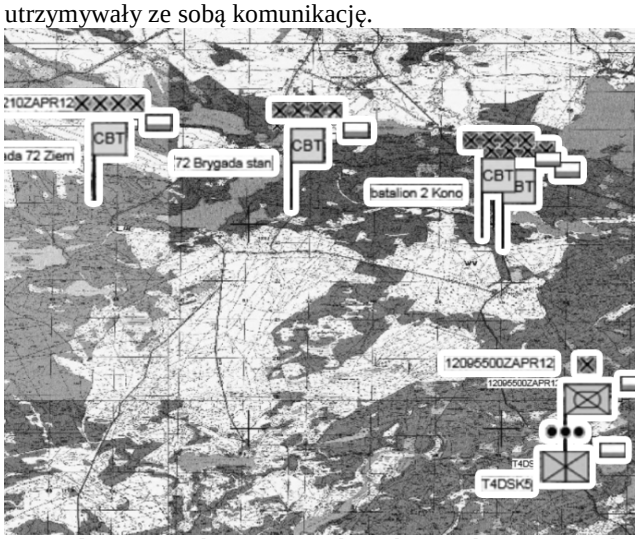
- Anteny zewnętrzne:
  - UPLOAD: do 400 kbit/s
  - DOWNLOAD: do 240 kbit/s
  - net speed test: 134-169 kbit/s
- Anteny wewnętrzne (siła sygnału ok. ½):
  - UPLOAD: do 200 kbit/s

- DOWNLOAD: do 140 kbit/s
- net speed test: 67-85 kbit/s.

Sprawdzono również możliwości przesyłania video z użyciem klienta VLC jest możliwa - obraz przesyła się, ale wysyłany w oryginalnej rozdzielczości 320x240 (QVGA) 15fps jest odbierany jako jedna klatka na kilkanaście/kilkadziesiąt sekund. Wysyłany w rozdzielczości 128x96 (SQCIF) 3fps jest odbierany płynnie.

W Polsce w sieci Orange średnie osiągi w sieci CDMA to 1-2 Mbit/s download i 200-400kbit/s upload. Orange CDMA oparte jest na relatywnie starej technologii. Nowoczesne sieci CDMA pozwalają na transfery rzędu 6-12 Mbit/s download i 3-9 Mbit/s upload, co w teorii wystarczy do przesyłania obrazu jakości HD w czasie rzeczywistym.

W ramach testu dokonano pomiaru zasięgu łączności. Analiza dostępności sieci CDMA (modemy dostarczyła firma Nordisk) została wykonana na poligonie Drawsko-Pomorskie [2], czyli w terenie niedostępnym publicznie. Rysunek przedstawia położenie jednostek, który utrzymywały ze sobą komunikację.



Rysunek. 3 Mapa dostępności jednostek na poligonie Drawsko Pomorskie, źródło: opracowanie własne.

Podczas testów udało się zestawić połączenie i przeprowadzić wymianę danych z użyciem protokołu UDP pomiędzy trzema jednostkami organizacyjnymi wyposażonymi w terminale komputerowe.

3. ANALIZA PROTOKOŁÓW TRANSMISJI DANYCH

Podczas analiz wybranych potencjalnych środków łączności zidentyfikowano i przedstawiono następujące protokoły transmisji danych możliwe do zastosowania w projekcie [3][4][5]:

- IP,
- UDP,
- TCP.

Wybrane protokoły transmisji danych wraz z odpowiednimi środkami łączności muszą gwarantować osiągnięcie wymaganych parametrów do pracy systemu.
Protokół UDP [7][8][9] jest zwykle wykorzystywany przez programy, które służą do jednorazowego przesyłania małych ilości danych lub mają wymagania dotyczące czasu rzeczywistego. W takich przypadkach niskie wymagania organizacyjne i funkcje obsługi multiemisji protokołu UDP (na przykład jeden datagram, wielu odbiorców) są bardziej przydatne niż funkcje protokołu TCP [10][11][12][13].
Protokół UDP różni się wyraźnie pod względem usług i funkcji od protokołu TCP. W tabeli przedstawiono porównanie połączeń IP w zależności od tego, czy do transportowania danych jest używany protokół UDP, czy protokół TCP.

Tabela 2. Porównanie protokołów UDP i TCP [14].

UDP	TCP
bezpołączeniowy	połączeniowy
nie gwarantuje dostarczenia, potwierdzania i szeregowania danych	gwarantuje dostarczenie, potwierdzanie i szeregowanie danych
Szybki, mały narzut danych	Wolny, duży narzut danych
Transmisja do wielu użytkowników	Transmisja jeden do jeden

Na tym etapie projektu logicznym wydaje się wybór protokołów:

- IP - ze względu na konieczność integracji z siecią stacjonarną,
- UDP lub TCP - do transmisji danych w zależności od: wybranego środka łączności, mocy obliczeniowej i pamięci RAM zespołu czujników danych do monitorowania urządzeń Straży Pożarnej, liczby danych do przesłania i dostępnego

pasma oraz konieczności kontroli przesyłanych danych na poziomie protokołu lub aplikacji.

Ze względu na zebrane cechy protokołów wymiany danych, korzystne wydaje się być wybranie protokołu UDP i zapewnienie gwarancji dostarczenia danych do odbiorcy na poziomie aplikacji.

4. PODSUMOWANIE I WNIOSKI

W niniejszym artykule przedstawiono opis projektu pod kryptonimem "Monitoring" oraz wyniki testów potencjalnych środków łączności: 802.11g oraz CDMA. Z wyników testów widać, że zastosowanie wzmacniacza do nadawania tylko po stronie Access pointa nie skutkuje wzrostem zasięgu transmisji, gdyż uzyskuje się brak symetrii mocy pomiędzy nadajnikiem a odbiornikiem. Ponadto w artykule przedstawiono krótką charakterystykę protokołów transmisji danych pod kątem ich wykorzystania w projekcie. Ze względu na parametry i warunki pracy systemu najlepszym rozwiązaniem dla budowanego demonstratora wydaje się być wybór:

- środków łączności: CMDA oraz Wi-Fi,
- protokołu UDP do transmisji danych z zapewnieniem gwarancji dostarczenia danych na poziomie aplikacji.

Oczywiście architektura systemu zostanie poddana dalszej analizie pod kątem jego zabezpieczenia odnośnie wymiany danych na styku sieci [15][16], zabezpieczenia przed potencjalnymi atakami z sieci publicznej, które mogą zablokować jej działanie [17]. Ponadto zostaną przeanalizowane architektury bezpiecznych sieci teleinformatycznych pod kątem wykorzystania dobrych praktyk w budowanym systemie [18].

Projekt ma charakter pracy badawczo-rozwojowej i jest finansowany ze środków NCBiR.

Literatura

1. Wniosek nr 13087 "Monitoring"
2. Sprawozdanie z warsztatów łączności i informatyki ASTER'08, TELDAT - opracowanie własne
3. Sprawozdanie częściowe z zadania badawczego 15011210 projektu "Monitoring" - Identyfikacja i rozpoznanie możliwych do wykorzystania środków transmisyjnych
4. http://swiatlan.pl/protokoly/protokol-ip.html, online 2014.07.23
5. http://technet.microsoft.com/pl-pl/library/cc785220(v=ws.10).aspx, online 2014.07.23
6. http://rejestrowanie-multimediow.eprace.edu.pl/135,Protokol_TCP.html, online 2014.07.23
7. Stevens W. Richard „UNIX: programowanie usług sieciowych", WNT, Warszawa 2002
8. Douglas Comer „Sieci komputerowe: intersieci", WNT, Warszawa 2000
9. Bruce Hallberg „Sieci komputerowe, kurs podstawowy", "Edition2000", Kraków 2001
10. Douglas E. Comer „Sieci komputerowe TCP/IP. Zasady, protokoły i architektura", WNT, Warszawa 1997
11. Craig Hunt „TCP/IP – administracja sieci", Oficyna Wydawnicza Read Me, Warszawa 1996
12. Nowicki K. Woźniak J. „Sieci LAN, MAN, WAN – protokoły komunikacyjne", Wydawnictwo Postępu Technicznego, Kraków 1998
13. Sprawozdanie częściowe z zadania badawczego 15011210 projektu "Monitoring" - Eksperymenty badawcze nowych technologii
14. Sprawozdanie częściowe z zadania badawczego 15011210 projektu "Monitoring" - Analiza protokołów wymiany danych na łączach radiowych
15. Apiecionek Ł., Romantowski M., Śliwa J., Jasiul B., Goniacz R., Safe Exchange of Information for Civil-Military Operations, MCC 2011: Military Communications and Information Systems Conference, Amsterdam, 17-18.10.2011, w: Military Communications and Information Technology: A Comprehensive Approach Enabler. Pod redakcją Marka Amanowicza. Warszawa: Redakcja Wydawnictw Wojskowej Akademii Technicznej, 2011. ISBN 978-83-62954-20-9, s. 39-50 (MK-312)
16. Apiecionek Ł., Romantowski M., Secure IP Network Model, Computational Method in Science and Technology 19(4) 209-213 (2013), DOI:10.12921/cmst.2013.19.4.209-216
17. Apiecionek Ł., Czerniak J., Zarzycki H., Protection Tool for Distributed Denial of Services Attack, Beyond Databases, Architectures, and Structures Communications in Computer and Information Science Volume 424, 2014, pp 405-414
18. Apiecionek Ł., Romantowski M., Security solution for Cloud Computing, Journal of Information, Control and Management Systems, Vol. 11, 2013, No. 2, ISSN 1336-1716