NIEZAWODNOŚĆ TRANSMISJI DANYCH PROTOKOŁU UDP W ELEKTROENERGETYCZNYCH SYSTEMACH TELETRANSMISYJNYCH WSPÓŁPRACUJĄCYCH Z SIECIĄ INTERNET

dr inż. Michał Porzeziński / Politechnika Gdańska
dr inż. Grzegorz Redlarski / Politechnika Gdańska

1. WPROWADZENIE

Obserwowany rozwój nowoczesnych technik mikroprocesorowych i informatycznych systemów przetwarzania danych na przestrzeni ostatnich lat związany jest bezpośrednio z rozwojem elektroenergetycznych systemów telekomunikacyjnych, opartych m.in. na technologii światłowodowej. Nowe rozwiązania znajdują wiele zastosowań praktycznych, począwszy od łączności w podsystemach telefonii stacjonarnej i mobilnej, poprzez transmisję danych w lokalnych sieciach komputerowych LAN (ang. *Local Area Network*), a skończywszy na procesach transmisji urządzeń pomiarowych i telemechaniki. Odgrywają zatem kluczową rolę podczas sterowania pracą systemu elektroenergetycznego, szczególnie z zakresu regulacji pierwotnej i wtórnej, sterowania dyspozytorskiego i elektroenergetycznej automatyki zabezpieczeniowej [3]. Ponadto z łatwością są wykorzystywane do zadań monitorowania stanu wielu układów i urządzeń tworzących strukturę systemu elektroenergetycznego (SEE).

W strukturze elektroenergetycznego systemu teletransmisyjnego wyróżnić można dwa obszary sieci: szkieletowej SDH/ATM (ang. *Synchronous Digital Hierarchy/Asynchronous Transfer Mode*) i dostępowej PDH (ang. *Plesiochronous Digital Hierarchy*). Urządzenia sieci szkieletowej są instalowane w ważniejszych placówkach SEE, takich jak rejony energetyczne czy centralna siedziba spółki, natomiast urządzenia sieci dostępowej są instalowane z reguły w stacjach i na posterunkach elektroenergetycznych. W obrębie sieci SDH/ATM stosuje się topologię fizyczną podwójnego pierścienia typu B-SHR, w tym rozwiązaniu połączenia fizyczne realizowane są równoległymi liniami światłowodowymi, wbudowanymi w przewody odgromowe OPGW (ang. *Optical Ground Wire*). W obrębie takiej topologii fizycznej stosowanych jest wiele technologii (np. STM-1, STM-4, STM-16) i standardów (np. łącza V.24, V.35, G.703) umożliwiających komunikację o różnych parametrach transmisji. W zakresie sieci PDH stosowane są rozmaite topologie fizyczne (np. magistrali, gwiazdy, siatki, pierścienia) oraz topologie logiczne (np. rozgłaszanie, przekazywanie tokena), które wspólnie odpowiadają za ciągłość i niezawodność procesów komunikacji [1, 2, 3].

Infrastruktura teleinformatyczna systemu elektroenergetycznego i ciągły rozwój nowoczesnych technologii, a także tendencje dążenia do zwiększania niezawodności pracy systemu elektroenergetycznego skłaniają do poszukiwania coraz nowszych i skuteczniejszych rozwiązań z tego zakresu. Prowadzone w wielu ośrodkach prace badawcze koncentrują się na licznych ważnych procesach zachodzących w SEE, dążąc do jak najlepszej ich realizacji. Niewątpliwie jednym z takich procesów jest proces automatycznej synchronizacji, którego nieprawidłowy przebieg może być źródłem wielu poważnych konsekwencji, zarówno prawnych, społecznych, jak i finansowych. Poprawę niezawodności tego procesu można uzyskać m.in. przez zwiększanie niezawodności urządzeń realizujących funkcję synchronizacji, jakimi są układy automatycznej synchronizacji prądnic (UASP).

Streszczenie

W artykule przedstawiono istotę niezawodności transmisji danych przesyłanych, w oparciu o zorientowany bezpołączeniowo protokół komunikacyjny UDP, w elektroenergetycznych systemach teletransmisyjnych, współpracujących z siecią Internet. Problematyka ta dotyczy szczególnie niewielkich (często bezobsługowych) obiektów elektroenergetycznych, w których proces monitorowania może być realizowany za pośrednictwem powszechnie dostępnej infrastruktury sieci Internet i odpowiedniego centrum monitorowania. Wskazano na najistotniejsze źródła błędów w procesie transmisji oraz możliwości częściowej ich eliminacji. Przedstawiono także opracowane i wykonane narzędzia diagnostyczne, metodologię i wyniki przeprowadzonych badań oraz najistotniejsze, wynikające z tych badań wnioski.

Nowoczesne UASP są zazwyczaj wysokiej klasy urządzeniami mikroprocesorowymi, a mimo to zdarza się, że ulegają rozmaitym awariom. Z kolei procesy diagnostyki tych urządzeń ograniczają się z reguły wyłącznie do tzw. przeglądów okresowych. Nie ma zatem możliwości ciągłego monitorowania ich aktualnego stanu, co byłoby możliwe po wyposażeniu UASP w odpowiednie oprogramowanie autodiagnostyczne, a czasem także interfejsy, umożliwiające współpracę z siecią komputerową. Wówczas informacja o stanie urządzenia mogłaby być bezpośrednio przekazywana np. do aplikacji znajdującej się w centrum monitorowania. Takie działanie wymaga jednak przeprowadzenia badań i realizacji opracowań, m.in. z zakresu sposobu przesyłu informacji pomiędzy badanym urządzeniem a aplikacją z dostępem do sieci Internet. Niewątpliwie jedną z podstawowych kwestii, jaką należy rozwiązać w tym zakresie, jest wybór protokołu komunikacyjnego i określenie skuteczności jego funkcjonowania.

Do transmisji danych w praktyce mogą być wykorzystywane różne protokoły komunikacyjne. Z uwagi na powszechność zastosowań, dwa spośród nich [5, 6]: TCP (ang. *Transmission Control Protocol*), którego format pokazano na rys. 1, i UDP (ang. *User Datagram Protocol*), którego format przedstawiono na rys. 2, zasługują na szczególną uwagę.

<table>
<tr><td colspan="2">Adres portu źródłowego</td><td colspan="2">Adres portu docelowego</td><td colspan="3">Numer sekwencyjny</td></tr>
<tr><td colspan="4">Numer potwierdzenia</td><td>HLEN</td><td>Zarezerwowane</td><td>Bity kodu</td></tr>
<tr><td colspan="4">Okno</td><td colspan="3">Suma kontrolna</td></tr>
<tr><td colspan="4">Wskaźnik pilności</td><td colspan="3">Opcje</td></tr>
<tr><td colspan="4">Uzupełnienie</td><td colspan="3">Dane...</td></tr>
</table>

Rys. 1. Format segmentu protokołu TCP

Adres portu źródłowego	Adres portu docelowego	Pole długości	Suma kontrolna	Dane...

Rys. 2. Format segmentu protokołu UDP

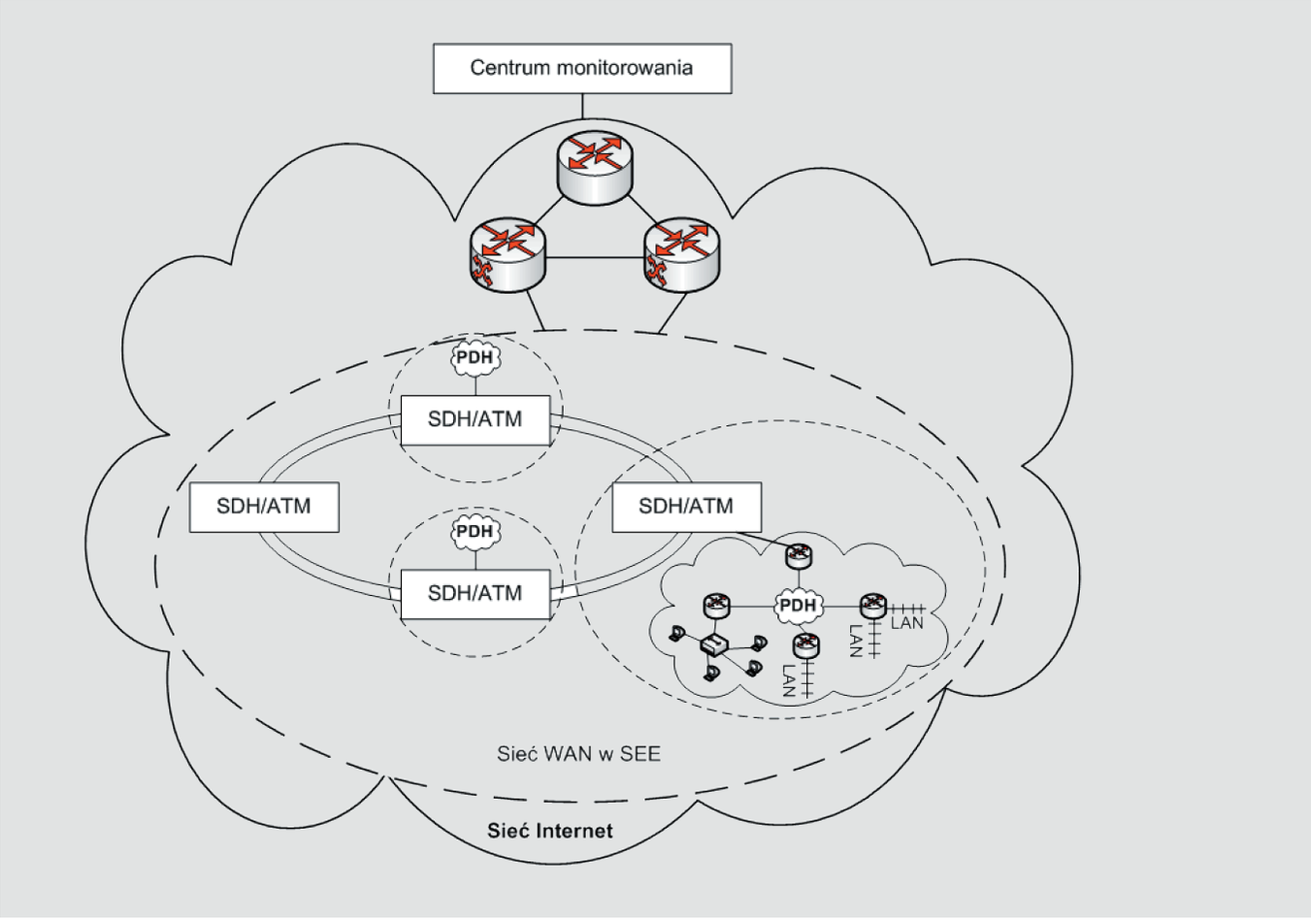
Definicje pól segmentów przedstawionych na rys. 1 i rys. 2 są następujące [1, 5, 6]:

- *numer portu źródłowego* – określa port wywołania, który może być punktem inicjującym połączenie
- *numer portu docelowego* – określa numer portu docelowego
- *numer sekwencyjny* – określa kolejność danego segmentu w ciągu danych dostarczanych do odbiorcy
- *numer potwierdzenia* – wskazuje na numer następnego, oczekiwanego oktetu danych
- *HLEN* – określa liczbę 32-bitowych słów, jakie występują w nagłówku segmentu danych
- *zarezerwowane* – pole z wpisaną wartością „0”
- *bity kodu* – pole pełniące funkcje kontrolne (np. dotyczące sposobu konfiguracji i zakończenia danej sesji)
- *okno* – pole warunkujące wielkość okna przesuwnego (w bajtach), jakie może zostać zaakceptowane przez urządzenie
- *pole długości* – określa w przypadku protokołu UDP długość pola danych
- *suma kontrolna* – pole warunkujące poprawność transmisji danych, na podstawie określonego algorytmu działania oraz informacji zawartych w polach nagłówka i danych
- *wskaźnik pilności* – określa miejsce warunkujące koniec przesyłu ważnych danych
- *opcje* – pole pozwalające zdefiniować maksymalny rozmiar segmentu TCP
- *dane* – pole właściwych danych, przesyłanych za pomocą protokołu TCP lub UDP.

Protokół TCP charakteryzuje się tym, że przed rozpoczęciem procesu transmisji ustanawia połączenie z urządzeniem docelowym w ramach procesu zwanego uzgadnianiem trójetapowym (ang. *Three-Way-Handshaking*) [1] oraz dodatkowo zawiera mechanizmy gwarantujące niezawodność transmisji danych, tj. numery sekwencyjne, numery potwierdzeń i okna przesuwne. Protokół UDP nie ustanawia połączenia z urządzeniem docelowym przed rozpoczęciem procesu transmisji i nie jest wyposażony w mechanizmy gwarantujące niezawodność. Stąd też w zorientowanym bezpołączeniowo protokole UDP konieczne jest zapewnienie odpowiedniego poziomu niezawodności transmisji na poziomie warstwy aplikacji. Natomiast, aby ten mechanizm był skuteczny i efektywny, konieczne jest oszacowanie prawdopodobieństwa występowania błędów transmisji i ich charakteru.

W praktyce często można spotkać sytuacje, kiedy do monitorowania stanu urządzeń pracujących na rozproszonych obiektach elektroenergetycznych, o niewielkich mocach znamionowych, wykorzystuje się sieć Inter-

net. Ponadto, niejednokrotnie, z powodu dużego kosztu tworzenia i utrzymywania wydzielonej sieci, w pewnych sytuacjach (np. gdy nie jest krytyczna niezawodność transmisji danych w czasie rzeczywistym) uzasadnione może być wykorzystanie do komunikacji publicznej sieci Internet. Stąd też, jeśli uwzględnić wydajną i „zamkniętą", a co za tym idzie, wysoce niezawodną strukturę teletransmisyjnej sieci elektroenergetycznej oraz konieczność transmisji danych pomiędzy tą siecią a centrum monitorowania przez powszechnie dostępne łącza sieci Internet (rys. 3), to szczególnie celowe i uzasadnione jest przeprowadzenie badań niezawodnościowych w sieci Internet, jeśli nie jest znana droga transmisji lub mogą wystąpić różnorodne czynniki zakłócające jej właściwą pracę.



Rys. 3. Ogólny schemat współpracy teleinformatycznej sieci WAN systemu elektroenergetycznego z siecią Internet

2. ŹRÓDŁA BŁĘDÓW TRANSMISJI UDP I PRZYCZYNY ICH POWSTAWANIA

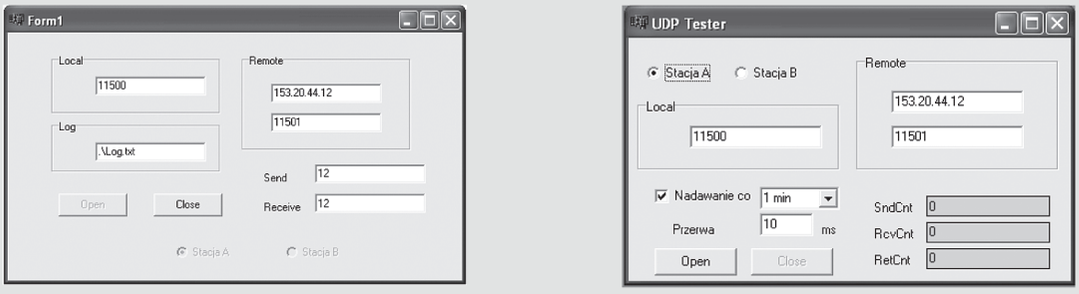
Potencjalne błędy powodujące utratę danych protokołu UDP związane są przede wszystkim z błędami przypadkowymi, powstającymi zwykle na poziomie warstwy fizycznej sieci komputerowej i z błędami urządzeń obsługujących wyższe warstwy protokołu. Na poziomie warstwy fizycznej sieci szczególnie istotną rolę odgrywają zakłócenia typu EMI i RFI, niewłaściwe funkcjonowanie urządzeń wchodzących w skład danej sieci, będące często skutkiem źle zaprojektowanej topologii fizycznej sieci, uszkodzenia mechaniczne torów transmisyjnych oraz źródła powodujące awarie zasilania.

Przyczyn nieprawidłowo zaprojektowanej topologii fizycznej może być wiele, jednakże do najpoważniejszych można zaliczyć: przekroczenie dopuszczalnych parametrów stosowanych mediów transmisyjnych (np. długości okablowania), nieprawidłową realizację połączeń kablowych (np. o zbyt dużej wartości impedancji przejścia), zbyt małą szerokość pasma transmisyjnego, czy stosowanie niewspółmiernych do wymagań urządzeń sieciowych. Czynniki te mogą stanowić przyczyny chociażby zwiększonej liczby kolizji w niejednej sieci, w efekcie czego może nastąpić nie tylko spadek wydajności sieci, ale również zwiększona utrata danych przesyłanych za pośrednictwem protokołu UDP [1, 2].

Uszkodzenia urządzeń sieciowych powodujące utratę transmisji często są związane z awariami interfejsów komunikacyjnych oraz awariami zasilania. Przywrócenie zbieżności sieci w takim przypadku wymaga określonego czasu, niezbędnego np. na wyszukanie innej (sprawnej) drogi transmisji. Ponadto utrata pakietów IP w urządzeniach sieciowych, takich jak przełączniki i routery, może być wynikiem nadmiernego obciążenia spowodowanego dużą liczbą przesyłanych danych w krótkim przedziale czasu i związanego z tym przepełnienia się ich wewnętrznych buforów.

3. NARZĘDZIA DO MONITOROWANIA PRACY SIECI

Badania niezawodności transmisji danych opartej na protokole UDP wymagają opracowania oprogramowania, które pozwoli na rejestrację wybranych parametrów transmisyjnych, na podstawie których możliwa będzie ocena określonego kanału transmisyjnego. Przykład takiego narzędzia stanowi opracowane i wykonane oprogramowanie o nazwie *TestUdp*, którego widok okien przedstawiono na rys. 4.



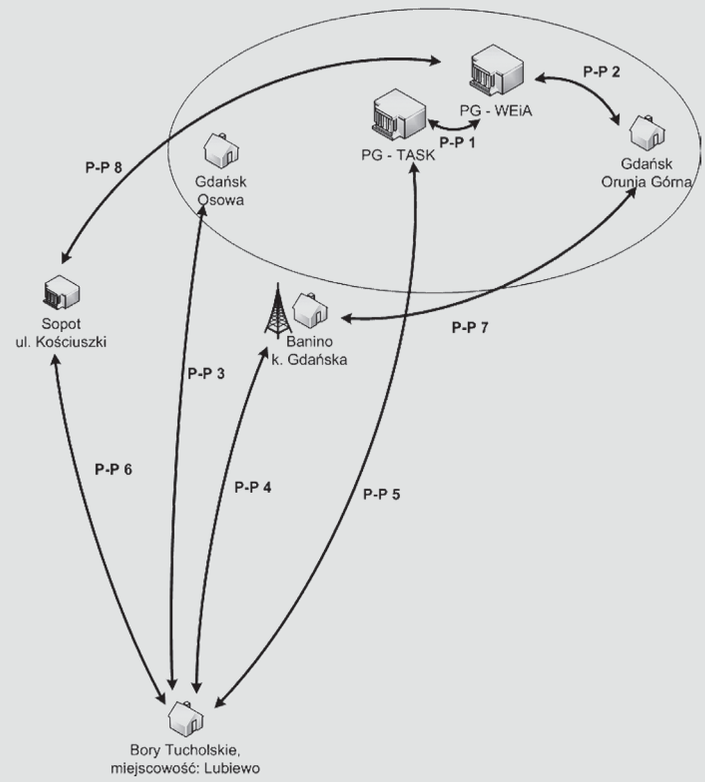
Rys. 4. Widok okien programu do monitorowania pracy sieci

Prezentowane oprogramowanie wykonano w dwóch wersjach. Pierwszej, która pozwala na wysyłanie kolejnych segmentów z 10-sekundowym interwałem czasowym, oraz drugiej, w której w jednakowych odstępach czasu (ze zdefiniowanym przez operatora czasem przerwy) wysyłane są trzy segmenty zawierające tę samą informację. Oprogramowanie wymaga uruchomienia w punktach diagnostycznych, pomiędzy którymi zachodzi proces transmisji danych. Jedna z aplikacji (Stacja A) pełni rolę hosta[1] nadawczego (lokalnego), a druga (Stacja B) rolę hosta odbiorczego (zdalnego), który odsyła odebrane dane z powrotem do nadawcy. Konfiguracja oprogramowania wymaga podania adresu IP hosta zdalnego oraz określenia numerów portów, które mają być wykorzystane w procesie transmisji. Liczba wysyłanych i odbieranych segmentów UDP wizualizowana jest w sposób ciągły w polach *Send* i *Receive* lub *SndCnt*, *RcvCnt* i *RetCnt* (w zależności od wersji oprogramowania). Szczegółowe informacje na temat uzyskanych wyników badań, tj.: czas transmisji, numer segmentu danych, opóźnienie transmisji oraz informacja na temat udanej lub nieudanej próby transmisji, gromadzone są w pliku tekstowym pełniącym rolę logu zdarzeń.

4. ANALIZA NIEZAWODNOŚCI TRANSMISJI UDP W SIECI INTERNET

Prowadząc badania, ograniczono się do kilku punktów węzłowych (rys. 5), pomiędzy którymi w różnych przedziałach czasu ustanawiano proces wymiany danych protokołu UDP. Zakres badań podzielono na dwa etapy. W pierwszym badano niezawodność transmisji na podstawie pierwszej z opisanych wersji oprogramowania. Za sytuację prawidłową uznawano pojedynczą transmisję danych, po której segment wysłany osiągał miejsce docelowe. Wyniki takich badań, dla połączeń oznaczonych symbolami P-P 1 do P-P 7 na rys. 5, przedstawiono w tabeli 1.

1 W terminologii sieci komputerowych wyrażenie *host* odnosi się do urządzeń posiadających kartę MAC, tzn. komputerów PC, terminali, serwerów itp.



Rys. 5. Mapa połączeń realizowanych podczas badań

Tab. 1. Wyniki analizy niezawodności transmisji danych opartej na protokole UDP

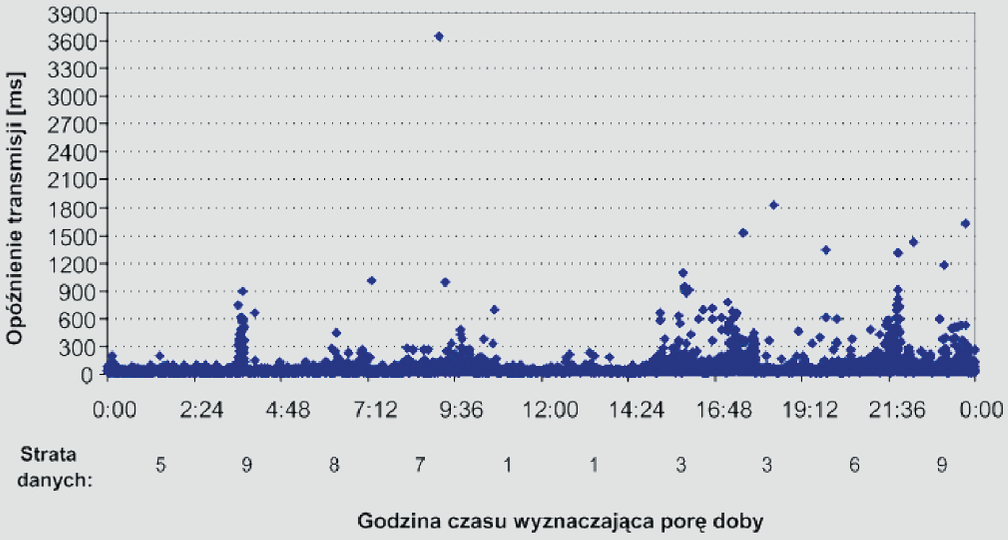
Nr połączenia (rys. 5)	Czas połączenia [hh:mm:ss]	Liczba danych	Liczba błędów (1/2/3/4/5)*	Liczba błędów [%]	Opóźnienie średnie [ms]	Opóźnienie maks. [ms]	Opóźnienie min. [ms]	Informacja o węzłach
P-P 1	23:32:10	8474	10 (5/0/0/0/1)	0,12	0,056	47	10	Sieć uczelniana – Sieć uczelniana
P-P 2	10:46:31	3817	38 (38/0/0/0/0)	0,99	2,003	4641	0	Sieć uczelniana – TV sieć kablowa
P-P 3	07:08:40	2597	11 (3/0/1/0/1)	0,42	186,49	1829	31	Neostrada TP – Neostrada TP
P-P 4	06:38:16	1969	148 (118/12/2/ 0/0)	7,52	200,67	1482	15	Sieć WiFi – Neostrada TP
P-P 5	02:07:31	766	1 (1/0/0/0/0)	0,13	38,56	250	31	Sieć uczelniana – Neostrada TP
P-P 6	50:17:31	18106	149 (142/2/1/0/0)	1,16	0,0612	78	0	Sieć uczelniana – Neostrada TP
P-P 7	26:03:23	9374	54 (54/0/0/0/0)	0,58	52,84	3650	15	Sieć WiFi – Neostrada TP

* Liczba błędów występujących kolejno po sobie: pojedynczych/podwójnych/potrójnych...

Na podstawie analizy wyników badań przedstawionych w tabeli 1 można stwierdzić, że mają one charakter losowy ze względu na wielkość opóźnienia transmisji i liczbę traconych segmentów UDP. Ponadto podczas wszystkich zrealizowanych procesów transmisji występuje zmienna liczba traconych danych UDP, która niewątpliwie zależy od aktualnego stanu łączy transmisyjnych. W różnych łączach występują także różne wartości opóźnień w procesach transmisji.

Uwzględniając powyższe czynniki, przeprowadzono dodatkowe badania z zakresu: zależności wielkości opóźnienia i liczby traconych segmentów danych, wpływu dodatkowo ustanawianych sesji transmisji z zakresu przesyłu tych samych segmentów danych na jakość transmisji oraz wpływu na jakość transmisji redundancji polegającej na zwielokrotnieniu liczby wysyłanych segmentów danych, zawierających tę samą informację.

Pierwszy z omawianych aspektów odniesiono do procesu transmisji oznaczonego symbolem P-P 8 na rys. 5, a uzyskane wyniki przedstawiono na rys. 6.



Rys. 6. Dobowa charakterystyka czasów opóźnienia transmisji i utraty danych UDP na przykładowym łączu w sieci Internet

Na podstawie rys. 6 można stwierdzić, że w godzinach zwiększonej aktywności na łączach (godziny pracy i pora wieczorna) występują większe opóźnienia w procesach transmisji. Ponadto w godzinach pracy (7:12––16:48) następuje znacznie mniejsza utrata danych (15 segmentów) niż poza tymi godzinami (37 segmentów). Analiza wyników pokazuje również, że większość błędów to błędy pojedyncze, związane najprawdopodobniej z przypadkową utratą danych. Należy się jednak liczyć również z możliwością występowania dłuższych przerw w funkcjonowaniu kanałów transmisyjnych, rzędu od kilkunastu do kilkudziesięciu sekund czy nawet minut.

Badając wpływ nadmiarowych kanałów (polegających na ustanawianiu dodatkowych sesji z zakresu przesyłu tych samych segmentów danych) na jakość transmisji, ograniczono się do przykładowego łącza P-P 8. Wyniki badań dla N = 1, 2, 3, 4 torów redundantnych przedstawiono w tabeli 2 (oznaczenia postaci $C_N^{2N_i}$ i $C_N^{3N_i}$ reprezentują największą liczbę błędów w seriach: dwóch spośród czterech ustanowionych torów transmisyjnych i trzech spośród czterech ustanowionych torów transmisyjnych).

Tab. 2. Wpływ redundancji kanałów przesyłowych na jakość procesu transmisji UDP

Liczba danych	Maksymalna liczba błędów transmisji				Maks. opóźnienie transmisji [ms]
	$N_1 \vee N_2 \vee N_3 \vee N_4$	C_N^{2Ni}	C_N^{3Ni}	$N_1 \wedge N_2 \wedge N_3 \wedge N_4$	
18106	149	20	6	4	94

Z uwagi na zaobserwowany losowy charakter błędów transmisji (tab. 2) można stwierdzić, że skuteczną metodą poprawy niezawodności transmisji UDP jest utworzenie redundantnych kanałów transmisyjnych oraz powtarzanie informacji w odpowiednio dobranych odstępach czasowych. Najsilniejsze oddziaływanie występuje po zastosowaniu tylko jednego dodatkowego kanału transmisyjnego, wówczas liczba błędów transmisji maleje niemal o rząd wielkości (z zaobserwowanych 149 dla pojedynczego kanału do 20 w sytuacji z pojedynczym torem nadmiarowym).

Badając wpływ redundancji polegającej na zwielokrotnieniu liczby wysyłanych danych zawierających tę samą informację, ograniczono się również do przykładu łącza P-P 8. Do badań w tym przypadku wykorzystano wersję oprogramowania, której istota polega na wysyłaniu – w każdym cyklu transmisyjnym – trzech segmentów danych zawierających tę samą informację i przyjęciu założenia o poprawności transmisji, jeśli choć jeden z wysłanych segmentów osiągnie miejsce docelowe. Przerwa pomiędzy kolejnymi wysłanymi pakietami definiowana jest przez operatora w polu o nazwie „Przerwa", zaś czas pomiędzy kolejnymi pakietami zawierającymi informacje w polu o nazwie „Nadawanie co" (patrz rys. 4). Wyniki przeprowadzonych badań zamieszczono w tabeli 3.

Tab. 3. Wpływ redundancji przesyłanych segmentów na jakość procesu transmisji UDP

	Nastawy programu i wyniki badań			
Nadawanie / przerwa	10 s / 10 ms	10 s / 3 s	60 s / 10 ms	60 s / 3 s
Liczba danych	8655	8644	1438	1436
Liczba błędów	182	82	19	13
Liczba przerw transmisji	88	1	6	1
Zgodność pokrycia	Pełna			

Analizując dane zgromadzone w tabeli 3, można stwierdzić, że rozdzielenie w czasie redundantnych segmentów danych korzystnie wpływa na niezawodność procesu transmisji. W obu przebadanych transmisjach, tzn. dla czasów nadawania 10 s i 60 s oraz czasów przerwy wynoszących odpowiednio 10 ms i 3 s, liczba traconych segmentów danych jest mniejsza, kiedy czasy przerwy są dłuższe i wynoszą 3 s. Fakt ten spowodowany jest z reguły krótkotrwałymi zaburzeniami w kanale transmisyjnym, co oznacza, że jeśli kanał ten jest nieaktywny przez odpowiednio długi przedział czasu, to pomimo wysyłania trzech segmentów zawierających ten sam zestaw danych, w 10-ms odstępach czasu, nie osiągną one miejsca docelowego. Ponadto bardziej szczegółowa analiza danych zgromadzonych w logach programu pozwala dostrzec, że jeśli pojawiają się dłuższe przerwy nieaktywności kanału transmisyjnego, to występują one w sposób jednakowy we wszystkich logach programu, a zwiększenie przerwy pomiędzy redundantnymi segmentami danych nie jest w stanie niczego zmienić. O stopniu zaistnienia takiej sytuacji świadczy umownie przyjęty w tabeli 3 parametr o nazwie „Zgodność pokrycia". W rozpatrywanym przypadku długi czas nieaktywności kanału występował we wszystkich logach programu i trwał ok. 13 minut.

5. PODSUMOWANIE

Rozwijająca się dynamicznie infrastruktura publicznej sieci Internet może we współpracy z teletransmisyjną siecią WAN, funkcjonującą w systemie elektroenergetycznym, stanowić podstawę budowy niedrogich systemów monitorowania obiektów, które są rozproszone na dużym obszarze geograficznym [4]. Przeprowadzone przez autorów badania pokazały, że:

- jakość transmisji danych w oparciu o standardowy protokół UDP w badanych sieciach jest wystarczająca do realizacji zadań diagnostyki i monitorowania, w których wymagany czas reakcji jest rzędu minut lub nawet godzin
- z uwagi na możliwość występowania losowych błędów transmisji celowe jest dążenie do stosowania dodatkowych metod skutecznie poprawiających niezawodność procesu transmisji, którymi przykładowo mogą być: tworzenie redundantnych kanałów transmisyjnych oraz wysyłanie nadmiarowych segmentów danych zawierających taki sam zestaw informacji, w odpowiednio dobranych odstępach czasowych
- zagadnieniem wymagającym odrębnego opracowania jest ochrona przesyłanej informacji i zabezpieczenie systemu przed sabotażem ze strony innych użytkowników sieci.

BIBLIOGRAFIA

1. Cisco Networking Academy program, CCNA 1 and 2 Companion Guide, 3rd Edition. Cisco Systems Inc., 2004.
2. Cisco Networking Academy program CCNA 3 and 4 Companion Guide, 3rd Edition. Cisco Systems Inc., 2004.
3. Poradnik inżyniera elektryka, tom III, rozdział 7, opracowany pod kierunkiem prof. Zbigniewa Szczerby, Wydawnictwa Naukowo-Techniczne, Warszawa 2005.
4. Porzeziński M., Mazur L., Remote monitoring and control of technical systems using internet network technology, Proceedings of the IEEE International Conference on Technologies for Homeland Security and Safety TEHOSS, Gdańsk 2005.
5. http://www.ietf.org/rfc/rfc0768.txt (marzec 2009).
6. http://www.ietf.org/rfc/rfc0793.txt (marzec 2009).