Wykorzystanie telewizji kablowej do transmisji informacji w sieciach SCADA

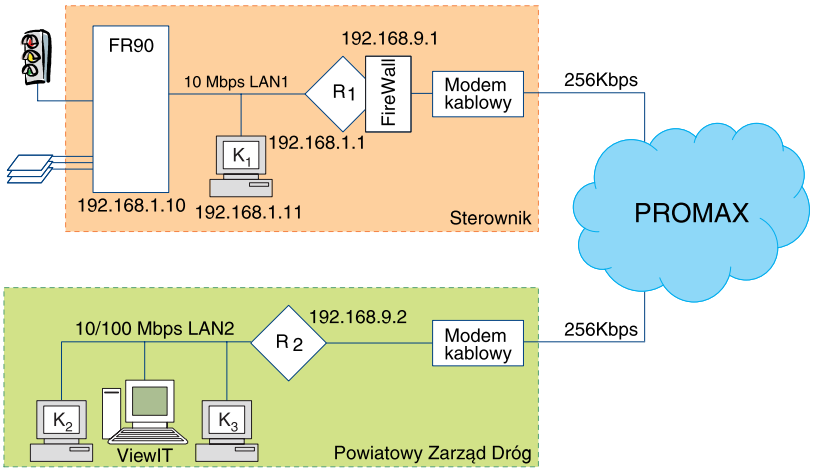
Tadeusz Nawalaniec

Telewizja kablowa jest kojarzona powszechnie z kanałami telewizyjnymi i z dostępem do Internetu. Jednak istnieją bardzo duże możliwości stosowania telewizji kablowej do przesyłania różnego rodzaju danych. Jedną z możliwości zastosowania telewizji kablowej są rozproszone systemy pomiarowo-kontrolne, których przykładem jest system sterowania sygnalizacją świetlną na skrzyżowaniach ulic.

W 2003 roku zainstalowano pierwszy w Ostrowie Wielkopolskim inteligentny sterownik sygnalizacji świetlnej CrossMaster FR90 firmy NH Polska. Na podstawie informacji pobieranych z zainstalowanych w jezdni detektorów podejmuje on decyzje dotyczące sterowania sygnalizacją świetlną na skrzyżowaniu. Sterownik ten ma również dodatkowe funkcje, tj. automatyczne dokonywanie pomiarów natężenia ruchu, zmianę programów sterowania oraz wiele innych. Jest to urządzenie, które może pracować autonomicznie, lecz dzisiejsza technologia wymusza tworzenie systemów monitorowania i zarządzania, umożliwiających zdalną obserwację i ingerencję w zachodzące procesy. Firma NH Polska udostępnia dwa tego rodzaju systemy: CrossMan firmy Vialis oraz uboższą wersję ViewIT własnej produkcji.

Rys. 1. Usytuowanie sterownika oraz centrum monitoringu

Mgr inż. Tadeusz Nawalaniec jest doktorantem w Instytucie Elektroniki i Telekomunikacji Wydziału Elektrycznego Politechniki Poznańskiej



Rys. 2. Struktura sieci telematycznej

Różne środki teletransmisji

Sterownik i aplikacja to jeszcze nie wszystko. Oba te składniki muszą się ze sobą komunikować. Istnieje wiele alternatywnych środków teletransmisji umożliwiających komunikację pomiędzy urządzeniami wykonawczymi a systemem zarządzająco-monitorującym. Ze względów kosztowych stosuje się najczęściej telefonię komórkową drugiej generacji, która podczas transmisji metodą CSD umożliwia przesyłanie informacji z szybkością 9.600 bit/s. Do przesyłania dużych ilości informacji warto zastosować tańsze w eksploatacji sieci trankingowe lub bardziej niezawodne linie telefoniczne komutowane bądź dzierżawione, zakończone modemami analogowymi lub cyfrowymi. To ostatnie rozwiązanie w najprostszej konfiguracji pozwala uzyskać szybkość przesyłania do 128 kbit/s, a z zastosowaniem technologii xDSL – nawet znacznie większą.

W Ostrowie Wlkp. zastosowano do tego celu – po raz pierwszy – telewizję kablową. Zdecydowano się na takie rozwiązanie ze względu na bardzo dobrze rozwiniętą w mieście infrastrukturę techniczną telewizji kablowej oraz niskie koszty podłączenia i eksploatacji. To nowatorskie rozwiązanie dedykuje zastosowanie wielu mechanizmów opisanych w tym artykule.

Usytuowanie sterownika oraz centrum zarządzania

Zarządcą drogi, na której zainstalowano sterownik Cross-Master FR90, jest Powiatowy Zarząd Dróg w Ostrowie Wielkopolskim. Odległość pomiędzy siedzibą PZD a sterownikiem wynosi ok. 4 km. Zdecydowano się na wykorzystanie dobrze rozbudowanej w mieście sieci telewizji kablowej dostarczającej również Internet. PZD korzystał już z usług informatyczno-telekomunikacyjnych tego operatora, zatem należało włączyć się jedynie do znajdującego się nieopodal sterownika sygnalizacji świetlnej okablowania operatora.

Struktura badanej sieci telematycznej

Telewizja kablowa

Telewizja kablowa PROMAX udostępniła dwa łącza o przepływności 256/512 kbit/s z Powiatowym Zarządem Dróg oraz 256/512 kbit/s – połączenie ze sterownikiem. Modem kablowy typ SB5100 firmy Motorola (własność telewizji kablowej) umożliwia przyłączenie urządzeń wykorzystujących standard 10Base-T.

Powiatowy Zarząd Dróg

Powiatowy Zarząd Dróg posiada swoją własną sieć lokalną LAN2. Za pośrednictwem routera R2 jest ona podłączona do sieci telewizji kablowej PROMAX. Na jednym z komputerów zainstalowano centralny system monitorowania i zarządzania ViewIT.

Sterownik

Sterownik sygnalizacji świetlnej CrossMaster FR90 wyposażono w system operacyjny czasu rzeczywistego OS-9. Aby umożliwić komunikację z modemem kablowym rozszerzono sterownik o dedykowaną mu kartę sieciową Ethernet typu M363 firmy Inducom Systems.

Ze względu na specyfikę sieci telematycznej PROMAX, niemożliwe było bezpośrednie podłączenie sterownika do modemu kablowego. Okazało się bowiem, że każde urządzenie końcowe podłączane do sieci PROMAX musi od niej dzierżawić adres IP za pomocą protokołu DHCP (*Dynamic Host Configuration Protocol*). Aby to spełnić, należałoby uruchomić w sterowniku klienta DHCP, co ze względów technicznych okazało się niemożliwe. Zdecydowano się zatem na wykorzystanie routera R1 typu DI-804V VPN Router firmy D-Link z zaimplementowanym mechanizmem klienta DHCP.

Po podłączeniu FR90 do routera R1 okazało się, że nie jest możliwe nawiązanie połączenia ViewIT – FR90. Podłączony do wewnętrznej sieci LAN1 sterownika komputer K1 z zainstalowanym serwerem/klientem TELNET dał następujące wyniki:

- możliwe było zainicjowanie stabilnego połączenia typu TELNET pomiędzy Powiatowym Zarządem Dróg a komputerem K1,
- możliwe było zainicjowanie stabilnego połączenia pomiędzy komputerem K1 a sterownikiem FR90.

Na tej podstawie udało się wyeliminować błąd sieci telewizji kablowej PROMAX oraz błędną konfigurację routera R1. Ze względu na możliwość zainicjowania połączenia wewnątrz LAN1 (w sterowniku) wyeliminowano również błąd komunikacji ze sterownikiem FR90 wewnątrz sieci LAN1. Sprawdzono zatem tablicę routingu w systemie OS-9:

```
Routing tables

Internet:
Destination        Gateway            Flags      Refs      Use  Interface
127.0.0.1          127.0.0.1          UH           10  1989207  lo0
192.168.1          192.168.1.10       U             3       15  enet0
192.168.1.10       127.0.0.1          UHS           0        0  lo0
```

Rys. 3. Standardowa tablica routingu

Na tej podstawie stwierdzono brak wpisu w tablicy routingu dotyczącego bramy (routera R1). Powodowało to, że wysyłane pakiety nie znajdowały w sieci LAN1 urządzenia o adresie docelowym IP, a system operacyjny sterownika nie wysyłał pakietów do bramy R1. Należało zatem uzupełnić wpis w następujący sposób:

```
Routing tables
```

Od tej pory wszystkie pakiety o adresach spoza LAN1 były kierowane do bramy (routera). To rozwiązanie okazało się poprawne, lecz niewystarczające, bowiem tablica routingu jest przechowywana w pamięci RAM-DRIVE i każde wyłączenie/włączenie zasilania powodowało ponowne ładowanie systemu operacyjnego, a co za tym idzie również standardowej tablicy routingu z pominięciem ww. wpisu. Rozwiązanie tego problemu wymagało dokonania odpowiedniego wpisu w plikach konfiguracyjnych, które są kompilowane na etapie programowania sterownika.

Bezpieczeństwo w sieci

Korzystanie z publicznej sieci telematycznej związane jest z ryzykiem. Sterownik sygnalizacji świetlnej jest urządzeniem bezpieczeństwa ruchu drogowego. Jakakolwiek ingerencja w sterownik mogłaby być niebezpieczna, zagrozić życiu lub zdrowiu. Bardzo ważna staje się zatem polityka bezpieczeństwa w sieci.

Dostęp do sterownika chroniony jest za pomocą mechanizmu autoryzacji (użytkownik + hasło). Jednak ze względu na czynnik ludzki, ten sposób zabezpieczeń jest często zawodny. Ponadto przy wykorzystaniu protokołu TELNET wszelkie informacje krążą po sieci w postaci jawnej, co powoduje, że przeciętny haker jest w stanie „podejrzeć" zarówno nazwę użytkownika jak i jego hasło.

Z tego też powodu zdecydowano się na wykorzystanie mechanizmu FireWall, który zaimplementowano w używanym routerze. Dzięki temu otrzymano następujące poziomy ograniczeń w dostępie do sterownika od strony sieci publicznej:

- poziom kierunku – zablokowano wyjście od strony sterownika, dzięki czemu wyeliminowano zagrożenia pochodzące od tzw. koni trojańskich;

- poziom adresów IP – dostęp do sterownika możliwy jest tylko z jednego adresu IP, co z mechanizmami zastosowanymi w sieci telewizji kablowej (ścisłe powiązanie adresu IP z adresem MAC) eliminuje możliwość włamania się z innego komputera niż zainstalowany w Powiatowym Zarządzie Dróg;
- poziom numerów portów – zablokowano wszystkie porty wejściowe poza 23 (usługa TELNET) i powiązano go z adresem IP Powiatowego Zarządu Dróg;
- poziom ICMP (*Internet Control Message Protocol*) – zablokowano odpowiedzi na zapytania typu PING, eliminując tym samym możliwość zablokowania przez hakerów routera poprzez generowanie wytężonego ruchu pakietów typu PING;
- poziom administracji routera – zablokowano możliwość zdalnej konfiguracji routera/firewalla od strony sieci publicznej, co wyeliminowało możliwość włamania się do tego urządzenia w celu zmiany konfiguracji.

Zastosowanie powyższej restrykcyjnej polityki bezpieczeństwa zminimalizowało niebezpieczeństwo związane z możliwością włamania się do sterownika od strony sieci publicznej telewizji kablowej. Skuteczność tego rozwiązania została następnie sprawdzona poprzez przeskanowanie wszystkich portów routera z innego (niż powiatowy) komputera w sieci.

Podsumowanie

Prace związane z wykorzystaniem medium jakim jest telewizja kablowa zakończyły się pełnym sukcesem. Przy wykorzystaniu mechanizmów bezpieczeństwa medium to okazało się być bardzo efektywne, bezpieczne i niezawodne. Ze względu na jego przepustowość możliwe jest również wykorzystanie go do celów monitorowania i zarządzania procesami ciągłymi szybkozmiennymi. Łącze to można porównać z dzierżawionym łączem telefonicznym, lecz jego efektywność, możliwości i przepustowość jest znacznie większa a koszty związane z eksploatacją znacznie niższe.

Telewizja kablowa przekazała do celów łączności ze sterownikiem FR90 pasmo o przepływności 256 kbit/s, które w chwili monitorowania jest wykorzystywane w 4 %. Pozostała część pasma, tj. ok. 246 kbit/s, nie jest używana. Oznacza to, że są możliwości rozszerzenia przedstawionego w artykule systemu o kolejne funkcje, takie jak przesyłanie obrazów ulicy z kilku nawet kamer przemysłowych bez utraty jakości systemu monitorująco-kontrolnego skrzyżowania.

Bibliografia

1. Amato V.: Akademia sieci CISCO, Wyd. MIKOM, Warszawa 2001.
2. Kupczak R. i in.: Rozproszona sieć pomiarowa na przykładzie stacji METEO z wykorzystaniem Internetu i telefonii GSM. Politechnika Warszawska, 24–26 czerwca 2001. Warszawa 2001 (Krajowy Kongres Metrologii, 27).
3. McCarty R.: CISCO WAN od podstaw, Wyd. MIKOM, Warszawa 2001.
4. Nawalaniec T., Urbaniak A.: Distributed System for Data Acquisition and Transfer to Information System of the Environment Monitoring. Technical University of Košice, 26–29 maja 2003. Tatranská Lomnica 2003 (International Carpathian Control Conference).
5. Nawalaniec T., Urbaniak A.: Wykorzystanie telefonii komórkowej drugiej generacji do przesyłu danych w systemach monitorowania środowiska. Polskie Zrzeszenie Inżynierów i Techników Sanitarnych, 30 listopada – 2 grudnia 2003. Wągrowiec 2003 (VI Ogólnopolska Konferencja Naukowo-Techniczna *Zastosowanie technik informacyjnych w zarządzaniu systemami wodno-kanalizacyjnymi* z cyklu Komputer w Ochronie Środowiska, 101).
6. Nawalaniec T.: Zintegrowany system GPS-GSM do monitorowania obiektu mobilnego, Politechnika Poznańska, Poznań 2001.
7. Nawrocki W.: Sensory i systemy pomiarowe, Wyd. 1, WPP, Poznań 2001.
8. Ogletree T.: Rozbudowa i naprawa sieci, Wyd. HELION, Gliwice 2002.

REKLAMA