STUDIA INFORMATICA 2003
Volume 24 Number 2B (54)

Robert WOJTAŚ, Rafał PRÓCHNICKI
Politechnika Szczecińska, Wydział Informatyki

ZASTOSOWANIA TECHNOLOGII INFORMATYCZNYCH W SYSTEMACH MONITOROWANIA ALARMOWEGO

Streszczenie. W artykule zaprezentowane zostały wybrane osobliwości systemów monitorowania alarmów, mające wpływ na poprawność ich działania. Jednocześnie zwraca się uwagę na możliwości rozwiązania występujących tam problemów poprzez zastosowanie dobrze znanych i przetestowanych rozwiązań stosowanych dotychczas wyłącznie w informatyce i telekomunikacji.

Słowa kluczowe: systemy alarmowe, systemy monitorowania obiektów, ochrona.

SOME PECULIARITIES OF THE COMPUTER TECHNOLOGIES IN ALARM MONITORING SYSTEMS

Summary. This article describes some peculiarities of alarm monitoring systems. For security and information consistency reason some communication functions used by the conservative alarm monitoring systems could be replaced by well known solutions used by the computer science and the telecommunication.

Keywords: security systems, alarm monitoring systems, security.

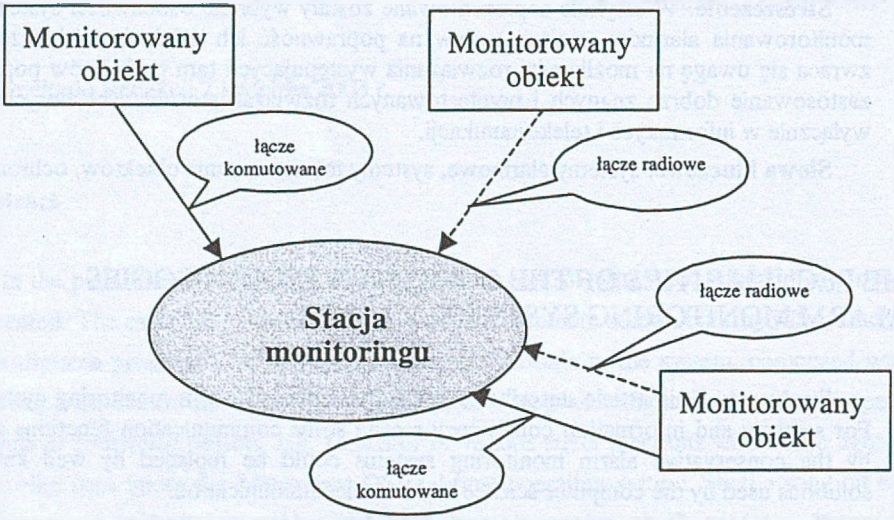
1. Wstęp

Systemy monitorowania alarmowego (włamaniowe, pożarowe, monitorowania środowiska itp.) stają się coraz bardziej rozbudowane. Konieczność instalowania takich systemów jest coraz powszechniejsza, rosną także wymagania co do funkcji, jakim mają one sprostać. Jednak wdrażanie nowych technologii w tej dziedzinie jest niestety bardzo wolne, co wynika z konieczności zapewnienia niezawodnej pracy takich systemów, stąd też duży konserwatyzm stosowanych rozwiązań. Jednak nowe wyzwania stawiane przed tymi systemami obnażają ich słabości w zakresie możliwości komunikacyjnych, jak i bezpieczeństwa. Dlatego też chcemy

przedstawić pewne rozwiązania umożliwiające poprawę tego stanu poprzez zastosowanie technologii informatycznych.

2. Obecny stan systemów monitorowania alarmów

W chwili obecnej najczęściej spotykaną strukturą systemów monitorowania jest struktura, w której wiele rozproszonych chronionych obiektów komunikuje się za pomocą łączy radiowych, czy też telekomunikacyjnych (łącza komutowane lub stałe) z jednym centralnym punktem, zwanym stacją monitorowania. Taką strukturę prezentuje rysunek 1. W stacji tej odebrany sygnał poddawany jest obróbce, a następnie, w zależności od zainstalowanego oprogramowania, w różny sposób prezentowany pracującym tam operatorom.



Rys. 1. Schemat obecnych systemów monitorowania
Fig. 1. Current structure of alarm monitoring system

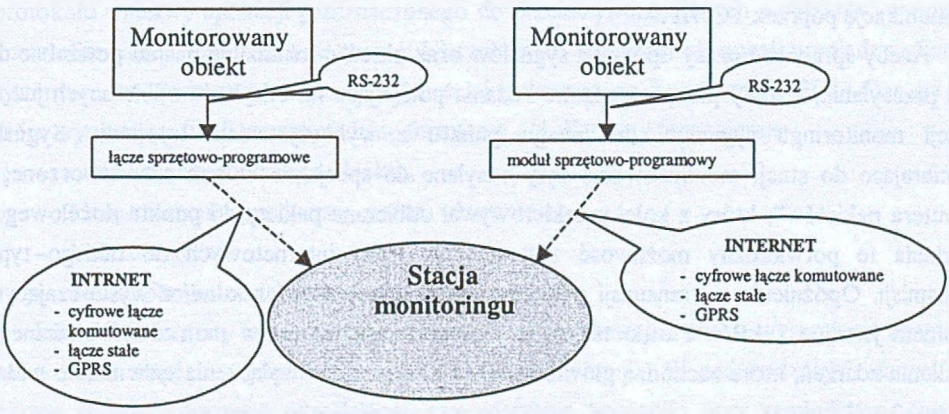
Na słabość obecnie istniejących systemów składa się kilka elementów. Niewątpliwie najsłabszym ich elementem w chwili obecnej są używane systemy transmisji danych. Dane z monitorowanych obiektów zazwyczaj przesyłane są "otwartym tekstem", a jeśli już stosowane jest utajnienie danych, to opiera się ono na metodach łatwych do zaimplementowania w prostych systemach sprzętowych (np. scrambling, zmiana częstotliwości), co przy obecnie powszechnie dostępnych urządzeniach jest zbyt łatwe do złamania. Umożliwia to zakłócenie transmisji, generowanie fałszywych kodów alarmowych, co daje możliwość wprowadzenia chaosu do systemów monitorowania. Kolejnym aspektem stanowiącym o słabości dzisiejszych systemów monitorowania jest przesyłane z obiektu do stacji monitorowania niezwykle ubogich

komunikatów. Zawarte w nich dane nie zawsze pozwalają stwierdzić, co tak naprawdę dzieje się w monitorowanym obiekcie, ani nawet kiedy to zdarzenie nastąpiło.

Jeszcze jeden problem występujący w większości przypadków systemów alarmowych polega na tym, że zainstalowane w obiektach urządzenia obsługują komunikację jednokierunkową, tzn. mogą one przesyłać informację do stacji monitorowania. Nie ma tu jednak możliwości potwierdzenia jej dotarcia, nie mówiąc już o sterowaniu. Może się to wydawać dziwne, gdyż obecna technologia pozwala na opracowanie rozwiązań bardziej nowoczesnych, a przecież od tych systemów w ogromnym stopniu zależy bezpieczeństwo ludzi i ich mienia.

3. Propozycja zmiany w systemach monitorowania

Proponowane przez nas zmiany prezentuje rysunek 2. Jak z niego wynika, główną innowacją jest opracowanie dodatkowego modułu sprzętowo - programowego, stanowiącego swoisty interfejs pomiędzy systemem alarmowym w obiekcie a stacją monitorowania. Głównym zadaniem interfejsu jest zapewnienie komunikacji w oparciu o protokoły rodziny TCP/IP oraz wykorzystanie infrastruktury klucza publicznego. Jest to najrozsądniejsze rozwiązanie pozwalające na dostosowanie dotychczas używanych systemów alarmowych do proponowanych rozwiązań, z jednoczesną eliminacją obecnie występujących problemów. W przyszłości należy pomyśleć o pełniejszej integracji tych rozwiązań, czyli na wbudowaniu nowych mechanizmów bezpośrednio do urządzeń stosowanych w systemach monitorowania.



Rys. 2. System monitorowana z uwzględnieniem modułu sprzętowo-programowego
Fig. 2. The monitoring system structure with combined hardware-software component

Biorąc pod uwagę wzrastającą złożoność systemów alarmowych, a co za tym idzie wzrost ilości przesyłanych danych, konieczne jest zwiększenie pasma niezbędnego do ich transmisji,

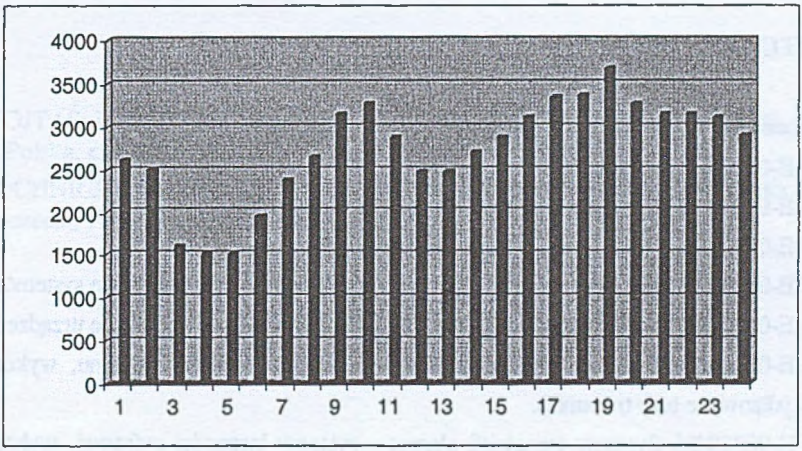
jak też zapewnienia odpowiedniej jakości połączeń komunikacyjnych, co obecnie, przy zastosowaniu technologii sieciowych, jest stosunkowo proste do uzyskania bez ponoszenia dużych kosztów.

W najprostszym przypadku interfejs sprzętowy stanowiłby zbiór standardowych komponentów (tj. procesor, pamięć itp.) wraz z odpowiednim oprogramowaniem. Już sama zamiana łączy komunikacyjnych na komunikację opartą na protokole IP pozwala na znaczną poprawę bezpieczeństwa w systemie. Poprzez bezpośrednie zastosowanie w komunikacji protokołu SSL lub też poprzez tworzenie łączy VPN rozwiązujemy problem otwartości transmisji w kanale komunikacyjnym. Prowadzenie wymiany danych z wykorzystaniem protokołu TCP pozwala na pewne przesyłanie danych w obu kierunkach. Dotychczas mało systemów monitorowania alarmowego zapewnia taką komunikację; aby zwiększyć pewność dostarczenia ramek do stacji, stosuje się wielokrotne nadawanie tych samych sygnałów, w nadziei że dotrą do adresata. Przy takim podejściu oprogramowanie pracujące po stronie stacji monitorowania musi być niewrażliwe na zbyt częste powtarzanie się tych samych danych z obiektów, a to z kolei może doprowadzić także do sytuacji niejednoznacznej oceny zagrożenia, co stanowi dodatkowe źródło przekłamań. Rozwiązanie takie zwiększa również obciążenie łącza komunikacyjnego. Protokół TCP daje gwarancję dostarczenia informacji lub też pozwala stronie nadającej na stwierdzenie, że transmisja danych zakończyła się niepowodzeniem. Skala stosowania rodziny protokołów TCP/IP jest w chwili obecnej tak duża, że stają się one standardem przemysłowym, czego dowodem jest już stosowanie ich w urządzeniach AGD, telefonach komórkowych itp. W związku z tym należy spodziewać się dalszego wyraźnego spadku cen podzespołów do produkcji urządzeń umożliwiających komunikację poprzez TCP/IP.

Ażeby sprawdzić czasy opóźnień sygnałów oraz określić minimalne pasmo potrzebne do ich przesyłania, zostały przeprowadzone badania polegające na odsyłaniu odbieranych już w stacji monitoringu sygnałów do innego punktu z wykorzystaniem Internetu. Sygnały docierające do stacji monitorowania były odsyłane do specjalnie w tym celu stworzonego „routera pakietów", który z kolei przekierowywał odbierane pakiety do punktu docelowego. Badania te potwierdziły możliwość zastosowania łączy internetowych do takiego typu transmisji. Opóźnienia w transmisji pakietów nie przekroczyły 5 sekund, a wystarczającym pasmem jest już 1 kB/s. Pasmo takie jest wystarczające, nawet w momentach znacznego nasilenia zdarzeń, które zachodzą głównie w chwili załączenia i wyłączenia systemu, co widać na rys. 3.

Rozwiązaniem problemu identyfikacji źródła sygnału jest zastosowanie powszechnie używanej i sprawdzonej infrastruktury klucza publicznego. Zapewnia nam to integralność, poufność, autentyczność i niezaprzeczalność przesyłanych danych, jak też współpracę z innymi podmiotami zaangażowanymi w ochronę obiektów (policja, straż itp.). Zastosowanie

infrastruktury klucza publicznego umożliwia nam szybkie wprowadzenie nowych rozwiązań bez konieczności dowodzenia ich poprawności. Na rynku istnieje bardzo dużo gotowych komponentów do budowy takich systemów, których zastosowanie gwarantuje dużą niezawodność i bezpieczeństwo. Dodatkowo w infrastrukturze klucza publicznego istnieje możliwość znakowania czasem, co pozwala jednoznacznie stwierdzić czas wystąpienia zdarzenia.



Rys. 3. Rozkład liczby odbieranych zdarzeń w ciągu doby
Fig. 3. Daily event count distribution

Kolejnym zadaniem wymagającym opracowania jest wprowadzenie nowego formatu danych wymienianych pomiędzy obiektem a samą stacją. Rozwiązaniem jest stworzenie protokołu warstwy aplikacji przeznaczonego do przekazywania danych z obiektów w postaci znormalizowanej i powszechnie znanej. Ułatwiłoby to wymianę informacji pomiędzy różnymi systemami monitorowania. Obecnie najczęściej stosowane są dwa formaty: SIA i Contact ID, które wypierają powoli starszą rodzinę formatów 4/2. Formaty te zawierają:

- numer monitorowanego obiektu;
- klasę zdarzenia (medyczny, pożar, włamanie);
- kod zdarzenia;
- źródło pochodzenia wewnętrz obiektu.

Jak widać, formaty te nie niosą w sobie żadnych informacji o czasie wystąpienia zdarzenia ani o stanie obiektu w momencie zaistnienia tego zdarzenia. W nadchodzących danych nie można znaleźć informacji określającej, czy zdarzenie wystąpiło przy zamkniętym, czy też otwartym obiekcie. Do opisu nowego formatu danych wymienianych w ramach systemu monitorowania proponuje się użycie języka XML, co zapewni dużą elastyczność i możliwość dowolnego rozszerzenia definicji systemów alarmowych.

4. Podsumowanie

Proponowane podejście uniezależnia systemy monitorowania obiektów od platform sprzętowych i programowych oraz zapewnia zgodność z przyszłymi możliwymi rozszerzeniami wymagań dotyczących systemów tej klasy.

LITERATURA

1. Schneier B.: Kryptologia dla praktyków. WNT , Warszawa 2002.
2. PN-E-08390-1 Terminologia.
3. PN-E-08390/11 Wymagania ogólne - postanowienia ogólne.
4. PN-E-08390/14 Wymagania ogólne - zasady stosowania.
5. PN-E-08390/51 Systemy transmisji alarmu - ogólne wymagania dotyczące systemów.
6. PN-E-08390/52 Systemy transmisji alarmu - ogólne wymagania dotyczące urządzeń.
7. PN-E-08390/54 Systemy transmisji alarmu - systemy transmisji alarmu, wykorzystujące specjalizowane tory transmisji.
8. PN-E-08390/55 Systemy transmisji alarmu - systemy łączności cyfrowej, wykorzystujące telefoniczną publiczną sieć komutowaną.
9. PN-E-08390/56 Systemy transmisji alarmu - systemy łączności akustycznej, wykorzystujące telefoniczną publiczną sieć komutowaną.

Recenzent: Dr inż. Dariusz Caban

Wpłynęło do Redakcji 28 kwietnia 2003 r.

Abstract

Most of contemporary alarm monitoring systems still uses inefficient and insecure communication methods based on direct connection to the central station by PSTN, radio or GSM network. Although direct transmission is a bit harder to intercept (excluding radio network of course) than transmission by public accessed medium, it is still possible to break the connection or to deceive the central station by sending false messages if you don't use other security means. There is also another drawback of these methods - low transmission speed, producing short messages containing as little data as it is possible. We propose to use another communication method based on standard TCP/IP link over public network, secured

by SSL, VPN and signing messages with electronic certificate. This way you can avoid all mentioned drawbacks. You need an universal interface between alarm system and communication medium. This could be made using standard hardware and software components. You need also a new transmission protocol allowing to send more data. We propose to use XML as the most flexible and extensible standard.

Adresy

Robert WOJTAŚ: Politechnika Szczecińska, Wydział Informatyki, ul. Żołnierska 49, 71-210 Szczecin, Polska, rwojtas@wi.ps.pl .
Rafał PRÓCHNICKI: Politechnika Szczecińska, Wydział Informatyki, ul. Żołnierska 49, 71-210 Szczecin, Polska, rprochnicki@wi.ps.pl .