Inteligentne Systemy Pomiarowe

Wykład 3

dr inż. Marek Wilkus
Wydział Inżynierii Metali i Informatyki Przemysłowej
AGH Kraków
http://home.agh.edu.pl/~mwilkus

Łączenie do Internetu

- Pomiary i Internet
- Protokoły
- Serwery
- Centralizacja
- Decentralizacja
- Federalizacja
- Bezpieczeństwo
- Praktyka – jak przebić NAT?
- Bezpieczeństwo użytkownika

Rys historyczny

- Od 1970 – Raportowanie pomiarów zakładów przez sieć dalekopisową.
- 1980 – Zarządzanie produkcją przez system podobny do BBS.
- 1990 – Eksperymentalne podłączenie urządzenia elektrycznego do Internetu (toster + miniaturowy komputer), z możliwością sterowania z zewnątrz (J. Romkey).
- ca. 1997 – Komercyjny streaming przez Internet,

Pomiary i Internet

+ Wyniki dostępne zawsze i wszędzie,
+ Możliwość zdalnego sterowania,
+ Łatwe lokalizowanie uszkodzeń,
+ Bardzo łatwa rozbudowa,
+ W przypadku jawności protokołu dowolna aplikacja kliencka.

- Konieczność dbania o bezpieczeństwo i regularnych aktualizacji,
- Warunki środowiskowe ("przebijanie" NATa) lub umowy trudne do przyjęcia.
- W przypadku naiwnego "poziomu decyzyjnego" uzależnienie od producenta jednego rozwiązania.

Model OSI

- Opisuje strukturę komunikacji w sieci urządzeń.
- Składa się z warstw, począwszy od sprzętu, skończywszy na aplikacjach, które wymieniają dane.
- Każda warstwa musi dysponować odpowiednim połączeniem ze sprzętem, siecią i resztą modelu, jak i wykorzystywać odpowiednie protokoły.

- **Warstwa fizyczna** - Fizyczne (elektryczne, optyczne, radiowe) sprzężenie urządzeń.
  - Standard opisuje również niezbędne parametry toru komunikacyjnego, elektroniczne składniki kart sieciowych itd.
  - W większości przypadków nadajemy binarne dane.

Model OSI (2)

- Warstwa łącza danych - ma na celu obsługę i jakościową kontrolę warstwy fizycznej.
  - Tworzenie odpowiednich ramek danych.
  - Zaopatrywanie ramek w sumy kontrolne i weryfikacja ich.
  - Sterowanie łączem.
  - Sterowanie dostępem do nośnika.
  - Współcześnie wspomagane sprzętowo.

Model OSI (3)

- **Warstwa sieciowa** - odpowiada za **trasowanie** ruchu oraz **enkapsulację** danych do pakietów. Odpowiada za znalezienie najlepszej drogi dla pakietów, zaadresowanych nagłówkami w warstwie łącza.
- **Warstwa transportowa** - Zapewnia spójne połączenie między stacjami, fragmentuje dane dla ich wysłania i składa odebrane.
  - Tutaj wykorzystuje się m.in. **TCP** i **UDP**.
  - Kontroluje ponawianie wysyłania brakujących pakietów.
  - Ponownie sprawdza integralność danych - po złożeniu z pakietów.

Model OSI (4)

- **Warstwa sesji** - Odpowiada za synchronizację danych różnych aplikacji. Przypisuje aplikacjom odpowiednie narzędzia komunikacyjne dostępne w systemie w celu zapewnienia stałości nawiązanych połączeń.
- **Warstwa prezentacji** - Przetwarza dane z aplikacji do postaci standardowej, dzięki czemu niezależnie od rodzaju aplikacji i użytych bibliotek niższe warstwy otrzymują dane w jednym, standardowym formacie.

Model OSI (5)

- **Warstwa aplikacji** - Najwyższa warstwa modelu - zapewnia mechanizm dostępu do łączności aplikacjom (procesy), mechanizmy łączności systemu w przestrzeni użytkownika (socket), obiekty sieciowe (procesy zdalne).
- Większość protokołów we współczesnych systemach wykorzystuje protokoły w warstwie aplikacji, a niższe warstwy są (mniej lub bardziej) standardowe.

Protokoły

- Współcześnie większość transportu danych pomiarowych jest realizowana tymi samymi protokołami co inne dane.
- Mikrokontrolery mają wystarczającą moc, by wysłać i przetworzyć proste zapytanie TCP, a nawet działać wyżej (HTTP).
- Mikrokomputery (RPi, jednoukładowe) – mogą tworzyć własne sieci i działać na zasadzie P2P.

Protokoły - przykłady

- Aplikacje o niskim priorytecie bezpieczeństwa:
  - Wysyłanie requestów za pomocą tekstu otwartego lub szyfrowania jednostronnego (niskie wymagania).
  - Na serwer można wysyłać nawet przez POST/GET.
  - Zatwierdzeniem lub odrzuceniem informacji zajmuje się serwer.

Protokoły - przykłady

- Aplikacje o wysokim priorytecie bezpieczeństwa, lecz wciąż komunikacja jednostronna:
  - Szyfrowanie komunikatów oparte o klucz urządzenia i sekret znany dwustronnie.
  - Przesyłanie własnym protokołem (lub fallback).
  - Możliwa dodatkowa autoryzacja.

Protokoły - przykłady

- Aplikacje o wyższym stopniu bezpieczeństwa, raportowanie i sterowanie:
  - Szyfrowanie komunikatów oparte o klucz urządzenia i sekret znany dwustronnie.
  - Zalecane generowanie/uzgadnianie kluczy szyfrujących.
  - Konieczna autoryzacja w celu uniemożliwienia podszycia się pod urządzenie.
- Unikać implementacji własnej kryptografii!

Serwery

- Najprostsze podejście: Serwer HTTP realizuje zapytania.
  - Możliwość prostej implementacji,
  - Do zaimplementowania wszędzie,
  - Dobrze udokumentowany
  - Problem: Przesyłanie dużej ilości danych
  - Problem: Średnia implementacja dla urządzeń o ograniczonych zasobach.

Serwery

- Dedykowany protokół (np. CoAP)
  - Przystosowany do konkretnego zadania,
  - Z reguły niewielkie ramki i mniejsze obciążenie,
  - Mogą go wykorzystywać niewielkie urządzenia,
  - Projektowany do sieci urządzeń.
  - Problem: Mniej implementacji,
  - Problem: Domyślnie szyfrowane RSA 3K.

CoAP

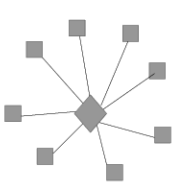
- Bezpieczeństwo: Typowa ramka:

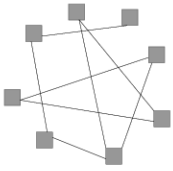
Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
4	32	Ver				Type				Token Length				Request/Response Code				Message ID															
8	64	Token (0 - 8 bytes)																															
12	96																																
16	128	Options (If Available)																															
20	160	1	1	1	1	1	1	1	1	Payload (If Available)																							

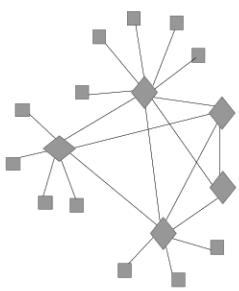
- Należy się autoryzować, ale czy nie da się przeciążyć?

Centralizacja, rozproszenie, federalizacja

- Jak wyglądać ma struktura systemu?







Centralizacja

- Jeden serwer (lub organizacja) zajmuje się przetwarzaniem danych.
  - Łatwiejsza kontrola administratorów nad danymi,
  - Możliwość szybkiego reagowania na anomalne zdarzenia,
  - Łatwa aktualizacja node'ów,
  - Konieczność zapewnienia znacznej nadmiarowości,
  - Przejęcie serwera = 100% kontroli

Centralizacja - zastosowanie

- Systemy gromadzenia/przetwarzania danych nie opuszczających przedsiębiorstwa,
- Systemy "Internet of things" – zysk z handlu danymi i profilami,
- Duże ujednolicone bazy danych, serwisy działające w WWW.
- Niekrytyczne systemy pomiarowe.

Rozproszenie

- Każdy węzeł wiąże się z kilkoma innymi, które wiążą się z kilkoma innymi, które…
  - Wysoka odporność na uszkodzenia,
  - Możliwość zapewnienia dużej nadmiarowości,
  - Wysoka niezależność węzłów,
  - Konieczność zapewnienia minimalnej liczby połączeń dla działania sieci,
  - Więcej połączeń – większe wymagania pasma – PROBLEM SKALOWANIA,
  - Problem zaufania.

Rozproszenie - zastosowanie

- Systemy wymagające nadmiarowości,
- Systemy odporne na cenzurę i manipulacje (np. TOR),
- Komunikatory (Chibiko), przesył plików P2P.
- Rozproszenie + kryptografia – bezpieczne przekazywanie wiadomości,
- Systemy pomiarowe oparte o "femtokomórki".

Federalizacja

- Każdy węzeł łączy się do „serwera” lub jest „serwerem”.
- „Serwery” działają w stopniu rozproszonym.
- Każdy węzeł może przesłać komunikat innym – przez „serwery”.
- Każdy „serwer” może realizować dodatkowe własne funkcje i od innych zależy na ile będzie to realizowane (konieczna zgodność protokołów).

- Przykłady: E-mail, Mastodon, SICOMP FMU

Federalizacja - zastosowanie

- Systemy odporne na awarie,
- Zdecentralizowane systemy komunikacyjne,
- Hierarchiczne systemy sterowania, pomiarów i raportowania.
- Systemy działające w „sieciach sieci”.

Istniejące systemy

- Połączenie sond pomiarowych do systemu realizuje się za pomocą **centralizowanej** architektury.
  - RS232,
  - Własne interfejsy przemysłowe,
  - Sygnały analogowe,
  - Sygnały multipleksowane z aparatury analogowej.
- Łączenie pomiędzy węzłami pobierania danych realizowane jest, w zależności od technologii, w sposób scentralizowany i hierarchiczny lub, w mniejszych sieciach, w sposób zdecentralizowany.

Istniejące systemy

- Przykład: Odczyt stanu aparatury produkcyjnej:
  - Pomiar napięć na istniejących przetwornikach.
  - Pomiar analogowy wartości konwertowany na cyfrowy za pomocą przetwornika potencjometrycznego lub multipleksowego.
- Zlokalizowany przy aparaturze interfejs koduje odczytane wartości i wysyła do sieci firmowej.
- Główny serwer otrzymuje gotowe dane do analizy lub wizualizacji.

Jak to zrobić?

- Bardzo często dokumentacja istniejących „końcówek” pomiarowych jest **niedostępna.**
- Wówczas pozostaje: Wymiana całości systemu (w środowisku np. rafinerii jest to raczej nieopłacalne) lub inżynieria wsteczna istniejących końcówek (bardzo pracochłonne).