Szyfrowanie transmisji sieciowej przy użyciu chaosu

Andrzej Chrzan
Paweł Gumola
Kamil Woźniak
Jakub Woźny

Politechnika Krakowska

Luty 2016

Plan prezentacji

Szyfrowanie

- Szyfr - funkcja matematyczna wykorzystywana do szyfrowania tekstu jawnego lub deszyfracji szyfrogramu. Zazwyczaj jedna funkcja wykorzystywana jest do szyfrowania, a inna do deszyfrowania wiadomości. Proces zmiany tekstu jawnego na szyfrogram nazywamy szyfrowaniem.
- Szyfrowanie - metoda zabezpieczenia transmisji danych przed ich ujawnieniem. Wdrożenie mechanizmów ochrony kryptograficznej gwarantuje integralność przesyłanych informacji oraz potwierdza, że druga strona komunikacji jest tą, za którą się podaje.

Szyfrowanie

Wyróżniamy 3 podstawowe obszary zastosowań szyfrowania danych

- łączenie sieci lokalnych oraz zapewnianie zdalnego dostępu pracowników do zasobów sieci lokalnej za pomocą szyfrowanych tuneli VPN (Virtual Private Network)
- zabezpieczanie stron WWW, usług poczty elektronicznej, telefonii internetowej, transferu plików lub komunikatorów internetowych przez szyfrowanie standardowych protokołów sieciowych w protokołach SSL (Secure Socket Layer) i TLS (Transport Layer Security)
- zapewnianie dostępu administracyjnego do serwerów przez protokół SSH (Secure Shell)

Teoria chaosu

Chaos deterministyczny - własność równań lub układów równań, polegająca na dużej wrażliwości rozwiązań na dowolnie małe zaburzenie parametrów. Dotyczy to zwykle nieliniowych równań różniczkowych i różnicowych, opisujących układy dynamiczne. Zachowanie takie można zaobserwować w wielu zjawiskach fizycznych, między innymi w zmianach pogody, oscylujących reakcjach chemicznych, zachowaniu niektórych obwodów elektrycznych i ruchu ciał oddziałujących grawitacyjnie.

Teoria chaosu - historia

- 1898 r. – Hadamard opublikował pracę dotyczącą bil poruszających się po powierzchni o ujemnej krzywiźnie bez tarcia. Pokazał on w niej, że trajektorie tych bil są niestabilne, oddalają się od siebie wykładniczo z dodatnim wykładnikiem Lapunowa.
- Początek XX wieku - Henri Poincaré pokazał, że w problemie n - ciał istnieją orbity, które są aperiodyczne, ale nie są zbieżne ani rozbieżne.

Teoria chaosu - historia

- 1961 r. – Edward Lorenz, uważany za pioniera teorii chaosu, przeprowadza analizy zjawisk pogodowych. Chcąc uprościć obliczenia przerwane błędem sprzętowym, zamiast przeprowadzać je od początku, rozpoczął kontynuację symulacji od wyników pośrednich uzyskanych przed momentem awarii. Jak zauważył pod koniec, otrzymane wyniki w znaczny sposób odbiegały od symulacji przeprowadzonych od początku do końca. Okazało się to skutkiem zaokrąglenia wprowadzanych ręcznie wyników. Równania okazały się zaskakująco czułe na niewielką zmianę warunków początkowych.

Chaotyczna transmisja danych

Transmisja danych wykorzystującą mapy chaotyczne była badana przez różnych autorów. Rozważamy symetryczną mapę namiotową f : [-1, +1] -> [-1, +1]

$$f(x) = \begin{cases} 2x+1 \\ \text{gdy } -1 \leq x \leq 0 \\ -2x+1 \\ \text{gdy } 0 \leq x \leq 1 \end{cases}$$

Jest to w zupełności chaotyczna mapa z niezmienną gęstością $\rho = 1/2/$ i wykładnikiem Ljapunova $\lambda = \ln(2)$. Mamy zatem iterację $x_{t+1} = f(x_t)$, gdzie t = 0,1, ... i $x_0 \epsilon [-1, +1]$, jest wartością początkową.

Chaotyczna transmisja danych

Generujemy ciąg o długości T z mapy, np. $x_0, x_1, ..., x_{T-1}$. Będzie to nadajnik. Mając teraz łańcuch bitów $b = (b_0, b_1, ..., b_{T-1})$ dla sygnału o długości T, gdzie $b_t[-1, +1]$, formujemy transmitowany sygnał $s = (s_0, s_1, ..., s_{T-1})$

$$s_t = b_t x_t, \text{ t=0,1,.....,T-1}$$

Odbiornik jest teraz dany jako

$$y_{t+1} = f(s_t), \text{ t=0,1,.....,T-2}$$

Chaotyczna transmisja danych

Oryginalną sekwencję bitów b może odnaleźć formując iloczyny

$$s_t y_t,\ \text{t=0,1,.....,T-1}$$

Jeśli $s_t y_t > 0$ to $b_t = 1$ i jeśli $s_t y_t < 0$ to $b_t = -1$. Oto dowód

$$s_t y_t = s_t f(s_{t-1})$$
$$= s_t f(b_{t-1} x_{t-1})$$
$$= s_t f(x_{t-1}) sinef(x_t) = f(-x_t)$$
$$= b_t x_t f(x_{t-1})$$
$$= b_t x_t^2$$

Chaotyczna transmisja danych

W konsekwencji

$$sign(s_t y_t) = sign(b_t x_t^2) = b_t$$

Schemat ten nie narzuca limitu długości ciągu bitów, ponieważ rozbieżność ciągu daje tylko lokalne błędy. Wartości s_t sekwencji są transmitowane i bezpośrednio operuje na nich odbiorca.

Chaotyczna transmisja danych

Inne chaotyczne mapy g o właściwościach g : [-1,+1] -> [-1,+1] i g(x) = g(-x) mogą także zostać użyte, tak jak mapa logistyczna

$$g(x) = 1 - 2x^2$$

Metody szyfrujące - reverse interval mapping

Jest to metoda, która koduje wiadomości w formie

$$m = m_1 m_2 ... m_n \epsilon \Sigma_2^*$$

Gdzie

$$\Sigma_2 := [0, 1]$$

$$\Sigma_2^* := \Sigma_2 U (\Sigma_2 x \Sigma_2) U (\Sigma_2 x \Sigma_2 x \Sigma_2) U ...$$

Wartości na przedziale [0,1] są związane z Σ_2 za mapą d : 0,1 -> Σ_2

$$d(x) = \begin{cases} 0 & \text{gdy } 0 \leq x \leq \frac{1}{2} \\ 1 & \text{gdy } \frac{1}{2} < x \leq 1 \end{cases}$$

Metody szyfrujące - reverse interval mapping

Na początku zaczynamy z dowolną wartością x_0 spoza przedziału [0,1]. Przykładowo $\frac{(1+r)}{2}$ jest wygodnym wyborem. Wartość ta oznacza początek wiadomości i koniec procesu dekodowania. Punkt ten posiada dwa odwrócone obrazy pod mapą r f

$$x_{1,0} = f^{-1}(\frac{x_0}{r}), x_{1,1} = 1 - f^{-1}(\frac{x_0}{r})$$

Każda z tych wartości leży po jednej stronie x $= \frac{1}{2}$, a zatem wybieramy wartość x_1 z przedziału $[x_{1,0}, x_{1,1}]$ spełniającą warunek

$$dx_1 = m_1 \ .$$

Metody szyfrujące - reverse interval mapping

Postępujemy w ten sam sposób aż do osiągnięci maksymalnej precyzji rejestru przechowującego wartość x_i albo do momentu, kiedy wszystkie wiadomości zostały zakodowane (np. po określeniu x_n). Zatem

$$x_0 := \frac{1+r}{2}$$

$$x_1 = \begin{cases} f^{-1}(\frac{x_0}{r}) \\ \text{gdy } m_1 = 0 \\ 1\text{-}f_{-1}(\frac{x_0}{r}) \\ \text{gdy } m_1 = 1 \end{cases}$$

$$x_2 = \begin{cases} f^{-1}(\frac{x_1}{r}) \\ \text{gdy } m_2 = 0 \\ 1\text{-}f^{-1}(\frac{x_1}{r}) \\ \text{gdy } m_2 = 1 \end{cases}$$