INTISARI

"Peningkatan Keamanan Pengiriman Data menggunakan Super Enkripsi BRC4 melalui Protokol DNP3 dalam Sistem SCADA"

Oleh
Eko Hadiyono Riyadi
16/405306/SPA/00563

Komunikasi antar perangkat pada *Supervisory Control And Data Acquisition* (SCADA) membutuhkan protokol jaringan *Distributed Network Protocol* (DNP3) yang merupakan protokol jaringan standar dan banyak digunakan dalam industri listrik dan air. Kelebihan DNP3 dibandingkan protokol yang lain adalah handal, efisien, dan efektif untuk transfer data *real-time* (waktu nyata). Pengiriman data yang masih asli (*plaintext*) melalui protokol DNP3 masih tidak aman dari serangan *interception* (intersepsi) karena nilai keacakan data transmisi rendah atau tidak ada.

Penelitian ini bertujuan untuk meningkatkan nilai keacakan data transmisi sehingga lebih aman dari serangan intersepsi. Kebaruan dan kontribusi penelitian ini adalah membangun metode super enkripsi BRC4 (Beaufort RC4) yang merupakan gabungan dari enkripsi Beaufort dan RC4, dilengkapi dengan pembangkitan empat kunci simetris dinamis. Pembangkitan kunci pertama merupakan kunci awal acak (K1) yang setiap sesi selalu berbeda, kunci kedua merupakan pembangkitan aliran kunci (K2) yang digunakan sebagai kunci Beaufort, pembangkitan kunci ketiga merupakan algoritma penjadwalan kunci (K3) dan keempat merupakan pembangkitan algoritma nilai acak semu (K4) yang digunakan sebagai kunci RC4.

Pengujian dilakukan dengan analisis ruang kunci, analisis korelasi dan analisis entropi. Besaran ruang kunci K1 mulai dari 2^{128} sampai 2^{2048} bit, sehingga aman dari serangan *brute force* (karena lebih besar dari 2^{100} bit). Nilai korelasi untuk metode usulan BRC4 pada data *instruction list*-1 (IL-1)=-0,010; IL-2=0,006; dan IL-3=0,001. *Pearson* menyatakan bahwa nilai korelasi semakin mendekati nilai nol artinya kedua data *ciphertext* dan *plaintext* semakin berbeda dan semakin acak. Sedangkan nilai entropi menunjukkan tingkat keacakan informasi dalam suatu paket data yang semakin mendekati nilai delapan, berarti data semakin acak dan semakin aman. Nilai entropi untuk IL-1 = 7,84; IL-2 = 7,98; dan IL-3 = 7,99. Jadi, metode usulan BRC4 mempunyai nilai korelasi lebih mendekati nol dan nilai entropi lebih mendekati delapan jika dibandingkan dengan hanya enkripsi Beaufort atau RC4 saja. Hal ini menunjukkan bahwa data *ciphertext* mempunyai nilai keacakan lebih tinggi jika dibandingkan dengan hanya enkripsi Beaufort atau RC4 saja, artinya lebih aman dari serangan intersepsi.

Kata kunci: Super enkripsi; BRC4; Kriptografi hibrid; Keamanan SCADA.

ABSTRACT

"Improvement of DNP3 Protocol Data Transmission Security using Super Encryption BRC4 in SCADA Systems"

by
Eko Hadiyono Riyadi
16/405306/SPA/00563

Communication between Supervisory Control And Data Acquisition (SCADA) devices requires the Distributed Network Protocol (DNP3), a standard network protocol widely used in the electricity and water industry. The advantages of DNP3 compared to other protocols are reliable, efficient, and effective for real-time data transfer. However, the data transmission that is still original (as plaintext) via the DNP3 protocol is insecure from interception and interruption attacks because the randomness value of the transmission data is low or non-existent.

This study aims to increase the randomness value of transmission data so that it is difficult to crack it from interception and interruption attacks. This research's novelty and contribution are to build the BRC4 super encryption method (Beaufort RC4), which is a combination of Beaufort and RC4 encryption, equipped with the dynamic symmetric four keys generation. The first key generation is the initial random key (K1) which is always different for each session; the second key is the generation of the keystream (K2), used as the Beaufort key, the third key generation is the key scheduling algorithm (K3), and the fourth is the pseudo-random value algorithm generation (K4) used as the RC4 key.

Tests are carried out by key space analysis, correlation analysis, and entropy analysis. The keyspace analysis results show the size of the keyspace ranging from 2^{128} to 2^{2048} bits, so it is safe from brute force attacks (because it is larger than 2^{100} bits). The correlation value for the proposed method BRC4 on the instruction list-1 (IL-1) data = - 0.010; IL-2 = 0.006; and IL-3 = 0.001. Pearson stated that the closer the correlation value to zero means that both ciphertext and plaintext data are increasingly different and random. Meanwhile, the entropy value shows the randomness of the information in a data packet getting closer to eight, which means the data is more random and secure. The entropy value for IL-1 = 7.84; IL-2 = 7.98; and IL-3 = 7.99. Thus, the proposed BRC4 method has a correlation value closer to zero and an entropy value closer to eight compared to just Beaufort or RC4 encryption alone. That shows that the ciphertext data has a higher randomness value when compared to only Beaufort or RC4 encryption, meaning that it is more secure from the interception attack.

Keywords: Super encryption; BRC4; Hybrid cryptography; SCADA security.