An Encryption Algorithm for End-to-End Secure Data Transmission in MANET

Abstract

Encryption is of prime importance when confidential data is transmitted over wireless network. Numerous encryption algorithms like AES, DES, RC4 and others are available for the same. The most widely accepted algorithm is AES algorithm. We have proposed a new algorithm based on the concept used by Rijmen and Daemen (Rijndael algorithm), the founders of AES algorithm. The proposed algorithm encrypts and decrypts two 128 bits data simultaneously i.e. 256 bits data, thus providing strong encryption accompanied with complex processing. The proposed Feistal algorithm uses various invertible, self-invertible, and non-invertible components of modern encryption ciphers and key generation same as that of AES. This algorithm provides a secure, fast, and strong encryption of the data. There is a huge amount of confusion and diffusion of the data during encryption which makes it very difficult for an attacker to interpret the encryption pattern and the plain text form of the encrypted data. The proposed algorithm is also resistant to Brute-Force and pattern attacks. This algorithm proves particularly useful while transmitting confidential data over a Bluetooth or wifi network. This algorithm is implemented in the Application layer of the device. The details of implementation are given in the article.
An Encryption Algorithm for End-to-End Secure Data Transmission in MANET

References

- Sakib, Rizwanul Karim; Reza, Bisway "Security Issues in VANET"; BRAC University Institutional Repository, April 2010
- Brent A. Peacock "CONNECTING THE EDGE: Mobile Ad-Hoc Networks (MANETs) for Network Centric Warfare"; Blue Horizons Paper, Center for Strategy and Technology, Air War College, April 2007

Index Terms

Computer Science Algorithms

Keywords

Encryption Algorithm Matrix Transformation Complement Feistal Dynamic Row Modification Row Column Swapping.