Düzce Üniversitesi Bilim ve Teknoloji Dergisi

Araştırma Makalesi

Kablosuz Ağlarda Yeni Bir Anahtar Dağıtım Yöntemi

Çağatay AY

Bilgisayar Mühendisliği Bölümü, Mühendislik Fakültesi, Düzce Üniversitesi, Düzce, TÜRKİYE
cagatayay@duzce.edu.tr

ÖZET

Ağ teknolojilerinin gelişimi ve dijital cihazların artışı multimedya iletimini hızlı ve kolay kılmıştır. Bununla birlikte açık haberleşme kanalları üzerinden yapılan dijital veri iletimi, telif hakkı ihlalleri, dolandırıcılık vb. birçok güvenlik açığını beraberinde getirmiştir. Bu sebepten dolayı güvenli veri iletimi için geliştirilen yöntem ve teknikler oldukça önem kazanmaktadır. Bu tekniklerden biri olan steganografi, gizli iletişim için zararsız görünen bir taşıyıcıya veri eklemesi yapan bilgi gizlemenin alt dallarından biri olarak tanımlanabilir. Veri gizlenirken kullanılan yöntem ve tekniğin sistem dışı kişiler tarafından bilinmesi güvenli veri iletişimini olumsuz yönde etkileyecektir. Steganografinin güvenlik konusunda yetersiz olması, beraberinde şifrelemeyi gündeme getirmektedir. Açık haberleşme kanalları ile yapılmak istenilen gizli iletişimin, çeşitli steganografik metotlar ve şifreleme algoritmaları ile desteklenmesi gerekmektedir. Bu çalışmada, ağ kanalları üzerinden güvenli anahtar dağıtımı için ağ steganografisinden yararlanan bir yöntem geliştirilmiştir. Deneysel sonuçlar, yapılan çalışmanın sağlamlık ve algılanamazlık koşullarında uygulanabilir olduğunu göstermiştir.

Anahtar Kelimeler: *Adaptive Huffman, AES, Ağ Steganografisi , Anahtar Dağıtımı, ICMP, Ping*

A New Key Delivery Method in Wireless Network

ABSTRACT

The development of networking technologies and the increase of digital devices have made multimedia transmission quick and easy. However, digital data transmission over open communication channels has introduced a number of security implications, such as copyright infringement and fraud. Due to this reason, the methods and techniques developed for secure data transmission gain importance. Steganography, one of these techniques, can be described as one of the subdivisions of information concealment, which makes data linkage to a carrier that seems harmless for occult communication. The methods and techniques of hiding data who are known by non system users will affect the secure data communication negatively. The inadequacy of the steganography on the security makes encryption important. The secret communication to be made with open communication channels needs to be supported by various steganographic methods and encryption algorithms. In this work, a method has been developed that utilizes network steganography for secure key distribution over network channels. Experimental results have shown that the work performed can be applied to the robustness and imperceptibility conditions.

Keywords: *Adaptive Huffman, AES, ICMP, Key Delivery, Network Steganography, Ping*

Geliş: 13/12/2016, Düzeltme: 14/12/2016, Kabul: 15/12/2016

*Bu makale, Düzce Üniversitesi Fen Bilimleri Enstitüsünde Doç. Dr. Resul KARA'nın danışmanlığında Çağatay AY tarafından yazılmış olan tezden üretilmiştir.