
**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.

# I. GİRİŞ

AĞ teknolojilerinin gelişimi ve dijital cihazların artışı multimedya iletimini hızlı ve kolay kılmıştır. Bağlantı hızının kullanıcılar için makul seviyelere çıkması, aynı oranda kablosuz ağların kullanımı da yaygınlaştırmıştır. Kablosuz ağların geniş bir şekilde kabul görmesi ve ihtiyacın artması, kablosuz ağların güvenliği ile ilgili bazı endişeleri de beraberinde getirmiştir. 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 [1].

Antik çağlardan buyana gizli haberleşme, gelişen teknoloji ile birlikte uygulama ve yöntem açısından farklılıklar göstermektedir. Gizliliğin oldukça önemli olduğu durumlarda iletilmek istenilen bilgilerin sistem dışındaki kullanıcıların eline geçmeden hedefe aktarılması amaçlanmaktadır.

Steganografi (steganography) olarak adlandırılan veri gizleme, iletişimin maskelenmesi ile elde edilen gizlilik ve güvenlik durumu olarak tanımlanabilir [2]. Kullanılan yöntemler ve şekil dikkate alındığında veri gizleme, şifrebilim (kriptoloji) ile yakından ilişkilidir. Veri gizleme sanatı olan steganografi ile şifreleme bilimi olarak adlandırılan kriptografi arasındaki en büyük fark, bilgiyi elde eden kişinin elde ettiği veri içerisinde önemli bir bilgi olup olmadığını fark edemiyor olmasıdır. Şifrelemede amaç, aktarılmak istenen mesajın anlaşılmaz hale getirilip, ara(gizli) anahtara sahip olmayan kullanıcıların orijinal mesajı elde etmesine engel olmaktır. Çözmesi zor olmasına karşın şifrelenmiş mesaj, ilgi çekici olması sebebiyle gizlenmiş veriyi belli etmektedir.

Kriptoloji, Yunanca krypto's (saklı) ve lo'gos (kelime) kelimelerinin birleşmesinden oluşmuştur ve haberleşmede şifre bilimi olarak tanımlanmaktadır [3].

Farklı iki birim arası haberleşmede, verinin güvenli şekilde aktarıldığından emin olmak gerekir. Aktarılmak istenen verinin şifrelenmesi güvenli haberleşmenin temelini oluşturmaktadır. Açık haberleşme kanalları kullanılıyorken sistem dışı kullanıcıların aktarılmak istenen gizli veriye ulaşabileceği, aynı zamanda bu veriyi bozup değiştirebileceği güvenli haberleşme için önemli bir problem olarak görülebilir [4].

Açık haberleşme kanalları ile yapılmak istenilen gizli iletişimin, çeşitli steganografik metotlar ve şifreleme algoritmaları ile desteklenmesi gerekmektedir. Gizli verinin steganografi ve şifreleme ile değişime uğraması bilgi gizlemenin temel prensiplerinden algılanamazlık ve sağlamlık açısından oldukça verimli sonuçlar doğururken, kapasite kavramını olumsuz yönde etkileyebilir. Elektronik ortamda iletişimin verimli ve hızlı olabilmesi aktarılmak istenen verinin boyutuyla ters orantılıdır. Hızlı ve etkili bir iletişim beraberinde sıkıştırmayı getirmektedir.

Gerçek zamanlı uygulamalarda bilginin aktarım zamanı oldukça önemlidir. Aktarılmak istenen verinin haberleşme öncesinde sıkıştırılması gerekir. Şifreleme ve steganografi metotları uygulanarak değişime uğrayan orijinal veriyi kayıpsız sıkıştırma algoritmaları kullanılarak sıkıştırmak, zaman ve kapasite tasarrufu sağlanmasına sebep olacaktır.

Bilgisayar tabanlı steganografik metotlar, gizli kanalı yapılandırmak için genellikle video, ses, resim ve metin gibi dijital medyalardan yararlanır. Son zamanlarda ağ protokolleri steganografik iletişim için yaygın olarak kullanılmaktadır. İçerisinde uygun ağ paketleri bulunan ağ protokolleri, steganografik iletişim için oldukça uygun bir ortam sağlamaktadır [5].

Bu alanda literatürde yapılan çalışmalar bakacak olursak; geliştirilen bir metotta IP paketinde bulunan TTL(Time to Live) alanı kullanılarak harici verinin paket içerisine yerleştirilmesi gerçekleştirilmiştir [8]. Sunulan bu metot, gönderilen son TTL'i tekrarlayarak '0' veya '1' kodlaması yapar. Bir diğer sunulan steganografik metotta Etherleak[9] güvenlik açığı kullanılarak ethernet veri paketine harici veri yerleştirme işlemi yapılmıştır [10]. Yapılan bir diğer çalışmada gizli kanal yapısı oluşturulurken IPID ve TCPISN alanları kullanılmıştır [11]. Ahsan ve ark. yapmış oldukları çalışmada gizli mesajın aktarılmasında IPID'in yüksek 8 bitini kullanmayı önermiştir [12]. Hintz, çalışan TCP protokolünü analiz etmiş ve TCP paketi içerisindeki URG alanını '0'a eşitleyerek gizli mesajı aktarmayı sağlamıştır [13]. Benzer bir çalışmada TCP paketinde yer alan TST alanı ve ICMP paketinde bulunan payload alanı gizli mesajın aktarılmasında kullanılmıştır [14]. Kablosuz iletişimde sıra kontrol ve parça kontrol gizli mesajın aktarılmasında kullanılmış diğer alanlara örnek olabilir [15].

Yapılan bu çalışmada, kablosuz ağlarda anahtar dağıtımı problemi ile başa çıkabilmek için ağ steganografisinden yararlanılmıştır. Ağı test eden ilk ping işleminde ilgili alıcıya anahtar gönderimi yapılarak başlangıç prosedürlerinin azaltılması amaçlanmaktadır. Anahtar verinin gönderimi sırasında veri bloğuna, şifreleme ve sıkıştırma gibi işlemler uygulanarak daha güvenli ve etkin bir dağıtım süreci gerçekleşecektir.

## II. ÖNERİLEN METOT

Bu bölümde, steganografi, sıkıştırma ve şifreleme teknolojileri kullanılarak gerçekleştirilen uygulama hakkında çalışma ilkelerine dair bilgiler verilip algoritma detaylı bir şekilde anlatılacaktır.

Yapılan çalışmada, kablosuz ağlarda anahtar dağıtımı ile ilgili oluşabilecek güvenlik problemleri ve zaman kayıplarını önlemek amacıyla ağ tabanlı uygulama geliştirilmiştir. Uygulama, dağıtılmak üzere kullanılacak anahtar verisini önce sıkıştırıp daha sonra şifreleyerek ağın durumunu test edecek olan ilk ping paketi içerisine gizlemektedir. Alıcıya aktarılan ping paketi üzerinde deşifreleme ve ayıklama gibi işlemler yapılarak anahtar dağıtımı gerçekleştirilmiştir.

### *A. GÖNDERİM*

Geliştirilen metotta kablosuz ağlarda anahtar dağıtım işlemi, algılanamazlık, sağlamlık ve bant genişliği gibi kavramlar dikkate alınarak 4 temel adımdan oluşmaktadır. *Veri Eşleştirme, Sıkıştırma, Şifreleme,* ve *Veri Modifikasyonu* gönderim aşamasının temelini oluşturan adımlardır.

Algoritmanın ilk adımı olan *Veri Eşleştirme* aşamasında anahtar veri, onaltılık formata dönüştürülüp elde edilen her bir değer için ping paketi içerisinde arama gerçekleştirilir. Bulunan konum değerleri bir dizi haline getirilip bir sonraki aşamaya aktarılmaktadır. Başka bir ifadeyle anahtar veri *K*, ve onaltılık dizi *A* şeklinde tanımlanacak olursa:

$$A = \{a_1, a_2, .. a_n\} = K_{16} \quad (1)$$

Daha sonra veri modifikasyonuna uğramamış orijinal ping paketi, onaltılık bir *P* dizisi şeklinde tanımlanır.

$$P = \{p_1, p_2, .. p_n\} \quad (2)$$

Bir sonraki aşamada, *A* dizisinin her bir elemanı *P* dizisi içerisinde aranıp konum bilgisi *I* dizisine kaydedilir.

$$I = \{i_1, i_2, .. i_n\} \quad (3)$$

Elde edilen *I*, bir sonraki aşamaya sıkıştırılmak üzere aktarılır. Anahtar veri kullanılarak oluşturulmuş *I* konum dizisi, gizli kanal aracılığıyla aktarılmak istenen anahtar veri uzunluğundan daha fazladır. Bu sebepten dolayı *Sıkıştırma*, gönderim aşamasının önemli bir adımını oluşturmaktadır. Sıkıştırma algoritmaları genellikle birbirini tekrar eden veriler üzerinde oldukça başarılı sonuçlar elde eder. İşte bu yüzden daha kısa uzunluk ve tekrar sayısı az olan anahtar verisi yerine, anahtar verinin paket içerisindeki konumu belirten dizi üzerinde sıkıştırma işlemi gerçekleştirilmektedir. Sıkıştırma işlemi, geniş kullanıma sahip ve güncel bir sıkıştırma algoritması olan Uyarlanır Huffman(Dinamik Huffman) ile gerçekleştirilmiştir. Bir önceki adımda elde ettiğimiz *I,* sıkıştırılarak aktarılmak istenen veri boyutu minimum seviyeye düşürülmektedir. Bir başka ifadeyle:

$$C = Compress(I) \quad (4)$$

Sıkıştırma işleminin ardından elde edilen *C*, aktarımın güvenli olabilmesi için bir sonraki aşamada *Şifreleme* işlemine alınır.

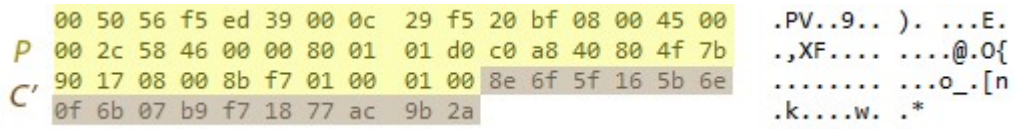
Sıkıştırılmış konum dizisi, *C* güvenli aktarım için şifrelenmeye ihtiyaç duymaktadır. Bu çalışmada günümüzde yaygın olarak kullanılan şifreleme yöntemlerinden biri olan AES(Advanced Encrytion Standart) algoritması kullanılarak ağ üzerinden güvenli parola aktarımı sağlanması amaçlanmıştır. AES blok şifreleme algoritmasını kullanılır. Veriler 4×4'lük diziler (matris) hâlinde bloklandıktan sonra uzunluğu en az 128 bit olan anahtarlar kullanılarak şifreleme gerçekleştirilir [6]. Yüksek hız ve düşük hafıza kullanımı nedeniyle yapmış olduğumuz bu çalışmada AES tercih edilmiştir. Bir başka ifadeyle açıklamak gerekirse:

$$C' = Encypt(C) \quad (5)$$

Sıkıştırılmış ve şifrelenmiş konum dizisi(*C'*), hazırlanan ping paketi(*P*) ile *Veri Modifikasyonu* aşamasında birleştirilir. Birleşim işleminin ardından paket alıcıya aktarılır ve anahtar teslimi gerçekleştirilmiş olur. Alıcı tarafında çeşitli aşamalardan geçecek olan ping paketi, çözümlenerek anahtar veri elde edilmiş olacaktır. Bir başka ifade ile:

$$P' = Concatenate(P, C') \tag{6}$$

Veri modifikasyonu sonrası alıcıya gönderilen ping paketi(*P'*) örneği Şekil 1'de gösterilmiştir.



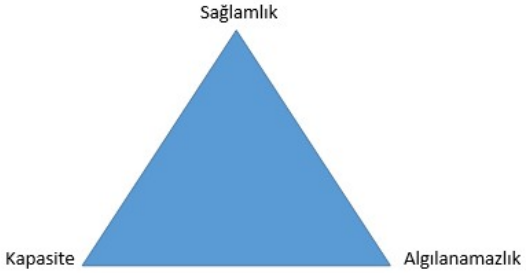

***Şekil 1.*** *Veri modifikasyonu sonrası oluşan ping paketi(P')*

*B. ÇIKARIM*

Çıkarım aşamasında ping paketi ile alıcıya ulaştırılan anahtar veri, gönderim aşamasında uygulanan yöntem ve tekniklerin çözme ve ayıklama adımları uygulanarak elde edilir. Çıkarım aşamasının ilk adımı *Veri Ayrıştırma*'dır. Bu aşamada ping paketi harici ve dâhili veri bloğu olmak üzere iki parçaya ayrıştırılır. Harici veri, şifrelenip sıkıştırılmış anahtar veriye ait konum bilgisini barındırırken dâhili veri, konum bilgisi bilinen anahtar veriyi içerisinde barındırmaktadır. İkinci aşama olan *Çözme* adımında harici veri deşifrelenerek sıkıştırılmış konum verisi elde edilir. Sıkıştırılmış konum verisi, algoritmanın bir sonraki aşamasında *Ayıklama* işlemine tabi tutularak anahtar veriye ait konum bilgisi elde edilir. Son aşama olan *Veri Eşleştirme*de konum bilgisi ile dâhili veri eşleştirilerek anahtar veri elde edilir.

## III. DENEYSEL SONUÇLAR

Bir steganografik sistem, farklı bakış açılarıyla değerlendirilmektedir. Bunlar, bilgi gizlenen örtü verisinin (cover object) ne kadar değiştiği, bilgi saklama kapasitesi ve sistemin dayanıklılığının ne kadar olduğudur [7]. Bir steganografik sistemin başarımını değerlendirmek için bu üç kritere bakılması gerekmektedir. Bu kriterleri steganografi ve steganaliz alanında çalışmaları olan bilim insanı Jessica Fridrich ortaya atmıştır ve Fridrich üçgeni Şekil 3'de gösterilmiştir.




***Şekil 2.*** *Fridrich üçgeni*

Günümüzde birçok steganografik metot vardır ve bu metotlara ait başarımların ölçülmesi için Fridrich üçgeni referans alınmalıdır. Her steganografik yöntem, algoritmik olarak farklı metotlar izlediği için farklı analiz metotları geliştirilmiştir. Bundan dolayı her metodun kendine özgü bir steganaliz metodu bulunmaktadır.

Etkili bir steganogram(steganografik nesne) elde etmede kapasite konusu oldukça önemlidir. Kapasite olarak yüksek miktarlarda veri biti gömmekten bahsedebiliriz. Yapılan deneysel çalışmada verilen anahtar uzunluğuna bağlı olarak kapasite ve entropi(düzensizlik) değerleri ölçülmüş, Tablo 1'de farklı anahtar uzunluklarına bağlı olarak değişen entropi, kapasite ve süre değerleri listelenmiştir.

***Tablo 1.*** *Farklı anahtar uzunluklarına ait süre, kapasite ve entropi değerleri*

| | **Anahtar** | **$t_I$** *(ms/tik)* | **I** *(byte)* | **$t_C$** *(ms/tik)* | **C** *(byte)* | **$t_{C'}$** *(ms/tik)* | **C'** *(byte)* | **P** *(byte)* | **Entropi** |
|---|---|---|---|---|---|---|---|---|---|
| 1 | Abc | 0/292 | 6 | 14/44319 | 6 | 29/89301 | 16 | 58 | 3,65 |
| 2 | Qwe123* | 0/791 | 14 | 16/48738 | 13 | 33/100681 | 16 | 58 | 3,62 |
| 3 | 12345 | 0/345 | 10 | 16/50517 | 8 | 29/89365 | 16 | 58 | 3,73 |
| 4 | 14531453 | 0/503 | 16 | 14/43112 | 9 | 31/96844 | 16 | 58 | 3,69 |
| 5 | 1*2A9-Test | 0/565 | 20 | 16/49068 | 19 | 29/89238 | 32 | 74 | 3,77 |
| 6 | 5321597532 | 0/709 | 20 | 13/40998 | 12 | 31/93908 | 16 | 58 | 3,78 |
| 7 | aftemelouchos | 0/935 | 26 | 15/46351 | 20 | 29/89940 | 32 | 74 | 3,79 |
| 8 | Loremipsum7725 | 0/924 | 28 | 12/38920 | 23 | 27/64310 | 32 | 74 | 3,91 |
| 9 | 12345678 | 0/660 | 16 | 12/37797 | 13 | 32/969993 | 16 | 58 | 3,50 |
| 10 | 16-11-1988 | 0/838 | 20 | 14/44467 | 14 | 27/82981 | 16 | 58 | 3,65 |

Tablo 1'de yer alan deneysel sonuçlarda süre, ms(milisaniye) ve tik(yazılımsal olarak ölçülebilen en küçük zaman birimi), kapasite ise byte olarak ölçülmüştür.

Elde edilen deneysel sonuçlara göre, veri eşleştirme ve veri modifikasyonu aşamaları yaklaşık 1 ms'de gerçekleşirken, karmaşık yapıya sahip sıkıştırma ve şifreleme aşamaları, anahtar uzunluklarına bağlı olarak ortalama 24 ms'de gerçekleşmektedir. Gerçek zamanlı uygulamalar dikkate alındığında kaydedilen süreler yeterlidir.

Deneysel sonuçlarda yer alan kapasite verilerine göre, birbirini tekrar eden semboller bulunduran anahtar örneklerinde sıkıştırma oranı yüksekken, anahtar uzunluğu ve tekrar eden sembol sayısı az olan örneklerde bu oran düşük kalmıştır. Sıkıştırma oranının düşük olması, sıkıştırma işleminin

başarısız olduğu anlamına gelmemelidir. Birbirini tekrar eden semboller içeren 14531453 anahtar verisine ait sıkıştırma oranı yaklaşık %50 iken, tekrarsız sembollerden oluşan 12345678 anahtar verisinde bu oran yaklaşık %20'dir. Bu oranlar sıkıştırma işleminin başarılı olduğunun göstermektedir.

AES şifreleme işleminde, sıkıştırılan veri uzunluğuna bağlı olarak 16 bayt ve 32 baytlık harici veriler elde edilmektedir. Varsayılan bir ping paketinde bu değer 32 bayttır. Deneysel sonuçlar göz önünde bulundurulduğunda örneklerin %70'i varsayılan 32 baylık paket genişliğinin altında kalmaktadır. Bu da etkin bant genişliği kullanımı olarak dikkat çekmektedir.

Yapılan çalışmada, ping paketine her seferinde 4 bit veri gizlemesi yapılmıştır. Bu değer aynı zamanda entropinin üst limitidir. Entropi kavramı ilk olarak Shannon tarafından bilgisayar bilimlerinde ve iletişiminde kullanılmıştır. Shannon Entropisi olarak da adlandırılan bu kavrama göre bir mesajı kodlamak için gereken en kısa ihtimallerin ortalama değeri, alfabede bulunan sembollerin logaritmasının entropiye bölümüdür. Alfabemizde 256 karakter olduğunu varsayarsak bu sayının logaritmasını mesajın entropisine böleriz. Mesajdaki değişim ne kadar fazla ise o kadar fazla koda ihtiyacımız olacaktır. Bilgisayar bilimleri açısından bir tanım yapmak gerekirse elimizdeki veriyi kaç bit ile kodlayabileceğimize entropi adı verilir. Bir bilginin entropisi hesaplanırken;

$$H = -\sum_{i=0}^{N-1} p_i \log_2 p_i \tag{7}$$

formülünden yararlanılmaktadır. Formüle göre, birbirinden farklı sembollerin sayısı *N*, o sembollere ait ihtimaller ise *p* olarak ifade edilmektedir.

Yapılan deneysel çalışmaya ait entropi değerleri karşılaştırıldığında, tüm değerlerin 4'e yakın olduğu gözlenmiştir. Entropi değerinin, yapılan çalışmaya ait üst limite(4 bit) yakın olması, orijinal mesaj (anahtar veri) ile gömülü mesaj arasında herhangi bir ilişkinin olmadığını anlamına gelir.

Daha önceden belirtildiği gibi güvenli bir steganografik tasarının istatistiksel olarak algılanamaz olması arzu edilir. Bu bölümde tarafsız bir değerlendirme için ping paketi içerisinde bulunan *data* bölümü incelenmiştir. Yapılan çalışmalar ve deneysel sonuçları neticesinde oluşturulan paket ile dağıtımı yapılacak olan anahtar veri arasında hiçbir ilgi olmadığı gözlenmiştir.

# IV. SONUÇ

Bu çalışmada, kablosuz ağlarda anahtar dağıtımı için yeni bir protokol-içi ağ steganografi yöntemi önerilmiştir. Bu amaçla anahtar dağıtımı, süreç içerisinde yer alan fazlalık prosedürleri ortadan kaldırmak ve sistem dışı kullanıcılar için dikkat çekici olmaması koşulları dikkate alınarak ping komutu ile gerçekleştirilmiştir. Gizli veri olan anahtar bilgisi, ilk aşamada Uyarlanır Huffman kodlama algoritması kullanılarak sıkıştırılmış, daha sonra günümüzde veri şifreleme standartı olarak kullanılan AES ile şifrelenmiştir. Son olarak sıkıştırılıp şifrelenen anahtar veri paket içerisinde *data* alanına gizlenmiştir. Böylelikle, önerilen metodun matematiksel karmaşıklığı arttırılmış ve gizlenen mesaj ile elde edilen çıktı arasındaki doğrusallık azaltılmıştır.

Deneysel sonuçlar dikkate alındığında entropi değerinin yüksek olması önerilen metodun algılanamazlık açısından yeterli olduğunu göstermiştir. Sıkıştırma ve şifreleme ile elde edilen harici verinin pakete gizlenmesi sonucu ping paketinin varsayılan boyutu azalmıştır. Böylelikle anahtar veri boyutundaki artış, ping paketinin kapasite değerini değiştirmemiştir. Devam eden çalışmalarda,

önerilen şemayı hızlandırmaya yardımcı olacak diğer şifreleme ve sıkıştırma algoritmalarının test edilmesi planlanmaktadır.

## V. KAYNAKLAR


[1] C. Chang, T. D. Kieu *Information Sciences* **180(16)** (2010) 3045-3058.

[2] B. Elci, S. B. Örs, V. Dalmışlı, *Bir Steganografi Sisteminin FPGA Üzerinde Gerceklenmesi*, **3. Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı**, Ankara-Türkiye, (2008) .

[3] B. Schneider, Applied Cryptography Second Edition, New York: John Wiley & Sons, Inc, 1996.

[4] A. Koltuksuz, *Elektronik Ticarette Güvenlik, Özgürlük Denetimi, Doğruluk, Bütünlük ve Sayısal İmza*, **4. Türkiye İnternet Konferansı**, İstanbul-Türkiye, (1998).

[5] G. Pipeleers *Systems & Control Letters* **58(7)** (2009) 510-518.

[6] C. H. Kim, *Differential Fault Analysis against AES-192 and AES-256 with Minimal Faults*, **2010 Workshop on Fault Diagnosis and Tolerance in Cryptography**, California-USA, (2010).

[7] W. Mazurczyk, M. Smolarczyk ve K. Szczypiorski *Telecommun Syst* **52(2)** (2013) 1113-1121.

[8] S. Zander, G. Armitage, P. Branch, *An empirical evaluation of IP time to live covert*, **15th IEEE International Conference on Networks**, Adelaide-Australia, (2007).

[9] O. Arkin, J. Anderson, http://leetupload.com/database/Misc/Papers/atstake_etherleak_report.pdf. *(Erişim Tarihi : 08th of August, 2016)*.

[10] B. Jankowski, W. Mazurczyk, K. Szczypiorski *K. Telecommun Syst.* **52(2)** (2013) 1101-1111.

[11] C. H. Rowland *First Monday* **2(5)** (1997).

[12] K. Ahsan, D. Kundur, *Practical data hiding in TCP/IP*, **Proc. Workshop on Multimedia Security at ACM Multimedia**, (2002).

[13] A. Hintz, *Covert Channels in TCP and IP Headers*, **DEFCON**, (2003).

[14] G. Fisk, M. Fisk, C. Papadopoulos, J. Neil, *Eliminating steganography in Internet traffic with active wardens*, **International Workshop on Information Hiding**, Berlin-Almanya, (2002).

[15] K. Szczypiorski *Telecommunication Systems* **49(2)** (2012) 255-259.