Kablosuz Ağlarda Güvenlik Artırımı: Kuantum Anahtar Dağıtım Protokolü Uygulaması

Umut Uygar[1]

[1] Gazi Üniversitesi, Bilişim Sistemleri, Ankara umut.uygar@gazi.edu.tr

Özet: Son zamanlarda kablosuz ağlar bilişim dünyasında gözle görülür bir önem kazandı. Bununla birlikte kablusuz ağlar için güvenli iletişim en büyük sorunlardan biri oldu. Kuantum anahtar dağıtımı, kriptografideki anahtar dağıtım sistemleri içerisinde, bilinen iki uç arasında gizli anahtar yayını için kullanılan yeni bir anahtar dağıtım sistemidir. Bu yöntem, iki uç arasında fizik kanunları ile garanti altına alımış güvenli bir iletişim kanalı sunarak kripto sisteminde anahtar dağıtımı problemini çözen bir kuantum kriptografisi uygulamasıdır. İletişim sadece kablolu değil kablosuz ortamda da oluşur. Kablosuz bir ortam olarak WLAN, kablolu olanlarla karşılaştırıldıklarında çok daha gürültülü ve genel olarak daha az güvenilirdirler.

Anahtar Sözcükler: 802.11 WLAN, Kuantum Anahtar Dağıtımı, Güvenlik.

Enhanced Security in Wireless Networks: Implementation of Quantum Key Distribution Protocol

Abstract: Recently, wireless networks have gained significant importance in computing world. As a result, providing secure communication for wireless networks has become one of the main concerns. Quantum key distribution is a new method in key distribution systems in cryptography which is used to broadcast secret key between two lawful parties. This method is a formation in quantum cryptography as part of the quantum mechanics which solves the key distribution problem in cryptosystem providing a secure communication channel between two parties with complete security guaranteed by the laws of physics. Communication not only occurs in wired medium but also in wireless medium. WLAN as a wireless medium are much noisier and less dependable in general than wired mediums.

Keywords: 802.11 WLAN, Quantum Key Distribution, Security .

1. GİRİŞ

Kablosuz yerel alan ağları gitgide daha popüler hale geldiğinden, işyerleri, hava alanları ve diğer ortak alanlarda çok daha fazla kullanılmaya başlandı.Bu LAN'lar, hem baz istasyonlu hem de baz istasyonsuz olarak iki konfigürasyonla da çalıştırılabiliyorlar. Yüksek hızları ve taşınabilir cihazlarda gösterdikleri yüksek kaliteli bilgi iletişimi performanslarıyla evlerde ve işyerlerinde kullanılmaya çok uygunlar. Yakın gelecekte iletişim endüstrisinin başı çeken aktörünün kablosuz teknoloji olacağı aşikardır. Kablosuz ağlar ve beraberinde gelen uygulamalar gün geçtikçe daha popüler olmakla birlikte, bununla beraber gelen güvenlik kaygıları da artmaya devam etmektedir. Kablosuz iletişimin doğasında var olan özelliklerden dolayı, herhangi bir saldırganın Denial Of Service (DOS) Attack, MAC Spoofing, ARP (Address Resolution Protocol) Poison gibi saldırılar gerçekleştirmesi çok daha kolay bir hale geldi.

Kablosuz iletişimde radyo dalgaları kullanıldığı için kablolu olanlarla kıyaslandığında araya girmelere ve saldırılara karşı çok daha kırılgan bir yapıları vardır. Hizmet popülerleştikçe, kablosuz teknoloji kullanıcılarının maruz kaldıkları risk de büyük oranda arttı. Hali hazırdaki kablosuz ağ protokollerinin ve kriptolama yöntemlerinin yüksek sayıda güvenlik riski olduğu bilinen bir durumdur. [6, 8]

Kuantum Anahtar Dağıtımı veya KAD (Quantum Key Distribution – QKD), özel anahtar bitlerinin iki parti arasındaki açık bir kanal üzerinden şekillendirilebildiği, güvenliği kanıtlanmış bir protokoldür. Anahtar bitleri, bu işlemden sonra klasik özel anahtar kriptolamasını kullanarak iki parti arasında güvenli iletişim için

kullanılır. KAD protokolü için tek koşul, kuantum bitlerinin açık bir kanal üzerinden, pozitif bir eşik değerinden daha düşük bir hata oranıyla iletilebilmesidir. Elde edilen anahtarın güvenliği kuantum bilgisiyle, dolayısıyla fiziğin temel kanunlarıyla garanti altındadır.

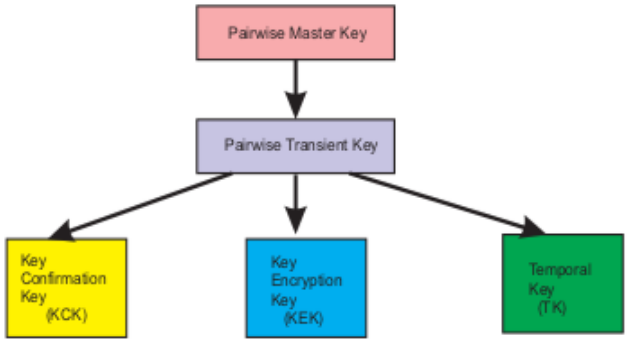
Klasik açık anahtar kriptografisi, biri özel diğeri açık olan asimetrik anahtarları kullanır. Kriptolama sürecinde gönderen istasyon, gönderimden önce bir açık anahtar kullanır. Alıcı istasyon ise, veri alımını takiben kriptoyu çözmek için karşılık gelen özel anahtarı kullanır. Her iki istasyonda kriptolama bilgisinin gereğini yerine getirebilmek amacıyla özel anahtarlarını gizli tutarlar. İstasyonlar, kendilerini diğer istasyonlara ya da erişim noktalarına tanıtabilmek amacıyla açık anahtar kriptografisini kullanabilirler. Bu klasik açık anahtar kriptografisinin en büyük açığı, özel anahtarın matematiksel olarak her zaman açık anahtarla bağlantılı oluşudur [14]. Yeterli kaynağa sahip olan her saldırganın açık anahtar sistemine saldırması mümkündür. Bu yüzden, açık anahtardan özel anahtar elde etme problemi matematiksel olarak ne kadar zor olursa olsun, bu sistemler saldırılara karşı herhangi bir anahtar güvenliğini garanti edememektedirler.

Kuantum kriptografisi sadece Kuantum Anahtar Dağıtımı (KAD) olarak bilinen anahtar üretimi ve tahsisi için kullanılır, herhangi bir veri mesajı yayını söz konusu değildir. Hali hazırda kullanılmakta olan BB84 [7], B92 [20] ve six-state [18] gibi KAD protokolleri vardır. Bunlardan BB84 diğerlerine göre biraz daha popülerdir ve birçok ağda yaygın olarak kullanılmaktadır [25]. Bu çalışma için BB84'ün bir varyasyonu olan SARG04 (Scarini, Acin, Ribordy ve Gisin) [21] kullanılacaktır

KAD hem optik hem de kablosuz ağlarda son zamanlarda oldukça büyük ilerlemeler göstermiştir. Bu konuda devam eden birçok araştırma projesi vardır, hatta şimdiden satışa çıkarılmış KAD ağları mevcuttur [17, 19, 26, 27, 28]. KAD çalışmamızda gönderici (Ayşe), anahtarı, kuantum kanalı üzerinden polarize fotonlar dizisi halinde alıcıya (Barış) gönderir.

2. IEEE 802.11 PROTOKOLLERİ

802.11 kablosuz ağları tarafından kullanılan protokollerin belli bir yapısı vardır. KAD protokolüne değinmeden önce IEEE 802.11 standardının tekrar gözden geçirilmesi gerekiyor çünkü burada kullanılan bazı standartlar aynen KAD protokolünde de kullanılmaktadır. IEEE 802.11'in güvenliği, protokole yapılan ilave bir düzenleme vasıtasıyla WEP (Wired Equivalent Privacy) olarak tanımlanmıştır [3]. Daha sonra WI-FI Birliği (WI-FI Alliance) tarafından WPA (Wi-Fi Protected Access) ve WPA2 tanımlanmıştır. IEEE 802.11'in, kendi ağlarındaki MAC (Medium Access Control) katmanında gelişmiş bir güvenlik sağladığı kabul edilir. Burada iki adet güvenlik algoritması sınıfı tanımlanır; Robust Security Network Association(RSNA) ve Transaction Security Network(TSN). IEEE 802.11, bu iki şifreleme paketine hitaben iki adet yeni gizlilik algoritması tanımlar; Temporal Key Integrity Protocol(TKIP) ve Counter Mode/CBC-MAC Protocol(CCMP) [12]. IEEE 802.11 yetkilendirme, anahtar yönetimi ve kullanıcı trafiği kontrolü gibi alanlarda geniş ağları koruma amaçlı, oldukça etkin bir çatı sunar. Geniş spektrumda bir yetkilendirme mekanizmasına olanak vermek için Extensible Authentication Protocol(EAP)[13] kullanır.



Şekil 1: Çift Temelli Anahtar Hiyerarşisi

Şekil 1'de çift temelli anahtar hiyerarşisi görülmektedir [3]. Çift temelli Ana Anahtar (PMK) yetkilendirme sunucusundan 802.11 yetkilendirmesi yoluyla alınır ve Pseudo Random Function (PRF) aracılığıyla çift temelli geçiş anahtarı (PTK) üretmek için kullanılır. PTK üç anahtara bölünür. İlk anahtar EAPOL Anahtar Doğrulama Anahtarıdır (KCK). KCK, EAPOL-Anahtar Değişimi (Key Exchange) tarafından verinin orijinindeki yetkilendirmeyi sağlamak için kullanılır. KCK, aynı zamanda mesaj bütünlük kodunu (Message Integrity Code – MIC) hesaplamak için kullanılır. İkinci anahtar EAPOL-Anahtar kriptolama anahtarıdır (KEK). KEK, EAPOL-Anahtar bağlantıları tarafından gizliliği sağlamak amacıyla vardır. KEK, GTK'yı (Group Temporal Key) kriptolamak için kullanılır. Üçüncü anahtar, unicast veri transferini kriptolamak için gizlilik protokolleri tarafından kullanılan TK (Temporal Key)'dır.

3. KUANTUM ANAHTAR DAĞITIMI

Kuantum Kriptografisi Kuantum Anahtar Dağıtımı (KAD), geleneksel kriptografideki sorunları çözmek amacıyla ortaya çıkmış yeni bir anahtar dağıtım tekniğidir. Bu teknik, güvenli iletişim vaadiyle kuantum mekaniği standardını kullanır. Birbirine karşı meşru durumdaki iki parti arasında, mesajın şifrelenip çözülebilmesi amacıyla sadece birbirleri için ve onlar tarafından tanınabilen rasgele bir gizli anahtar üretilmesine izin verir [14].

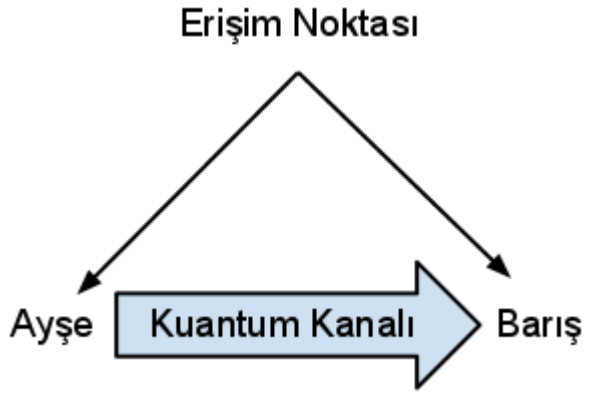
Kuantum kriptografinin en iyi yönlerinden birisi, üçüncü bir partinin veya bir dinleyicinin varlığını tanımlayabilmesidir, ki bu sayede anahtar bilgisine erişim zorlaştırılır. Bu, kuantum sisteminin genelinde yapılan bir ölçüm işleminden tüm sistemin etkilendiği kuantum mekaniğinin temel karakteristiğinin bir sonucudur. Üçüncü parti anahtarı dinlemeye çalıştığında mutlaka bir ölçüm işlemi yapmak zorundadır, bu da ortaya gözle görülür bir anomali çıkaracaktır.

Bir iletişim sistemi, kuantum çakışması ya da kuantum dolaşıklığı kullanılarak ve veri kuantum durumları içinde iletilerek üçüncü parti dinlemeleri fark edecek şekilde uygulanabilir. Dinlemeden kaynaklanan rahatsızlık belli

bir eşiğe ulaştığında ya da bu eşiği geçtiğinde iletişim durdurulur ve gizli anahtar üretimi yapılmaz. Tam tersi durumda, yani dinleme rahatsızlığı belirlenen eşiğin altında olduğunda bir anahtar üretilir ve iletişimin güvenliği garanti altına alınır [5].

Kuantum kriptografisi anahtar üretimi ve tahsisi için kullanılır, herhangi bir iletişim verisinin iletilmesinde kullanılmaz. Üretilen anahtar, mesajın şifrelenmesi ve açılması amacıyla, seçilecek herhangi bir klasik simetrik kriptografi tekniği ile birlikte, açık kanal (public channel) olarak bilinen standart iletişim kanalı üzerinden iletişimi gerçekleştirmek için kullanılır.

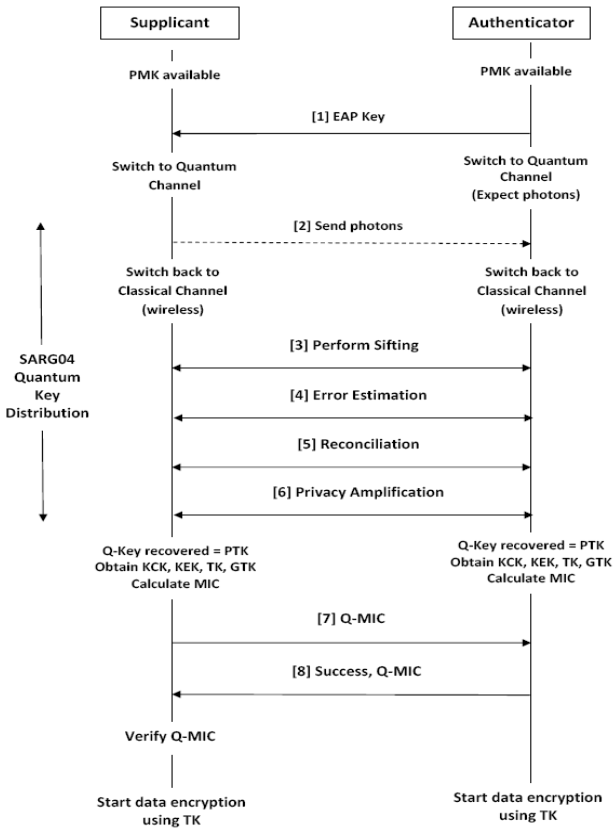
KAD, fotonları ya da bitleri alıcı ile verici arasında iletmek için kablosuz ortamı (havayı) kullanır. Bu kablosuz ortamın mesafesi uzadıkça, KAD'nin kalitesi düşmektedir. O yüzden uygulanabileceği uygun ortamlar ev/işyeri içi vb. mesafenin çok fazla uzamadığı ortamlardır.



Şekil 2: Donanımsal Uygulama

4. ÖNERİLEN PROTOKOL

Kablosuz ağların, GSM, GPRS, CDMA, CDMA/CD gibi birçok uygulama alanı vardır. WI-FI ağlar tarafından sağlanan kablosuz kaplama sadece 100m ile sınırlıdır. Özellikle hava alanlarında, restoran ve kafelerde oldukça popüler hale gelmişlerdir. Amacımız KAD kullanarak kablosuz ağlarda güvenli anahtar dağılımı yapmak olduğundan IEEE 802.11 (WI-FI) ailesinin bu amaca en uygun kablosuz ağlardan biri olduğu düşünülmektedir. Kuantum görevleri üzerinde etkisi olan çevresel şartlar minimuma indirilebildiğinden bu standart alanın uygun olduğu düşünülmektedir. Bu yeni protokolün iletişiminde genel olarak iki kanal kullanılır; Kablosuz Kanal (WI-FI) ve Kuantum Kanalı.



SARG04 Kuantum Anahtar Dağıtımı süreci, şekil 3'teki 3 ve 6 numaralı akışları arasında olduğu gibidir. İlk işlem olarak iletim kuantum kanalına geçer. İstemci, genişliklerini kullanarak ölçüm yapmak amacıyla tüm alınan fotonların izini sürer. Foton iletimi biter bitmez kablosuz kanal, protokolün diğer kısımlarının uygulanmaya geçebilmesi için sonlanır.

Şekil 3: Önerilen Protokol

İki parti tarafından da alınan anahtarlar dinleyici v.s. gibi etken durumlar yüzünden hatalar içerirler. KAD'nin birbirini takip eden üç aşaması, nihai güvenli anahtarı elde etmek amacıyla bu hataları silmeye çalışır. Eleme işlemi (sifting: 3 numaralı akış) yetkilendiriciyi kullanarak hatalı kaydedilen tüm bitleri siler. Hata tahmini ve düzeltme işlemi (4 numaralı akış), belirlenen eşik seviyesinin miktarını belirler ve iletişim devam eder.

Kuantum iletimi işlemin tamamlanabilmesi için, PMK'ya eşit ya da daha büyük bir kuantum anahtarının iyileştirilebilmesi amacıyla yeterli miktarda foton gönderdiğini garanti etmelidir. CCMP için PTK 256 bit, PMK için TKIP ise 384 bit kullanır. Bu yüzden bu aşamada kuantum anahtarındaki fazladan bitler kaydırılarak PTK İle aynı uzunlukta olması sağlanır. İşte bu kısaltılmış kuantum anahtarı PTK olarak kullanılır. PTK hazır olduğunda, PRF kullanarak diğer anahtarları da içeren anahtar sıralaması tekrar işlenebilir durumdadır.

PTK'dan KEK, KCK ve TK elde edilir. MIC ise KCK kullanılarak hesaplanır. Elde edilen MIC, müteakip protokol mesajlarında çift taraflı yetkilendirmede kullanılır. Bu aşamada istemci MIC ile PMK'nın eşit uzunluktaki ilk bitleri arasında XOR işlemi yapar. Bu işlem sonucu elde edilen MIC'e Quantum MIC (Q-MIC) denir.

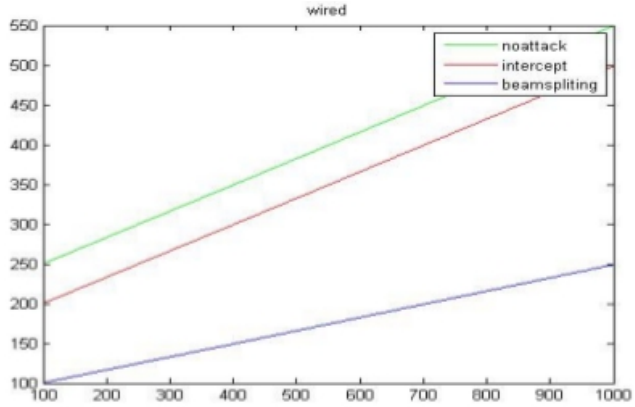
Q-MIC = (MIC) XOR (PMK'nın MIC uzunluğundaki ilk bitleri.

Q-MIC daha sonra istemci tarafından yetkilendiriciye gönderilir (Şekil 3; akış 7). Yetkilendirici Q-MIC'i doğrular. Yetkilendirici tüm anahtar hiyerarşisi bilgisine sahip olduğundan kendi MIC'ini hesaplar ve sonucu istemciden gelenle karşılaştırır. Uyum durumunda istemci yetkilendirilir. Son araştırmalar dört yollu anlaşmanın (4-way handshake) açıkları üzerinde yoğunlaşmıştır [5,6,8,16]. 4 yollu anlaşmanın ilk mesajının DOS saldırılarına açık olduğu kanıtlanmıştır. Saldırganlar, 4 yollu anlaşmanın bütün aşamaları bittikten sonra istemciye hiç durmaksızın 1 numaralı mesajı göndererek sistemin çökmesine neden olabilmektedirler. Burada anlatılan protokolün anahtar dağıtımı KAD ile

yapıldığından mesaj akışlarında bahsedilen değerlerin kullanılması gereksizdir. Kuantum iletimi için, normalde var olan donanımlar foton transferi gerçekleştirilebilmek amacıyla istemci ve yetkilendirici arasında Görüş Çizgisine (LOS – Line of Sight) ihtiyaç duyar. Bu alanda son zamanlarda birçok çalışma olmuştur ve artık böyle bir gereklilik yoktur. Bu çalışmaların en önemlilerinden biri Kedar ve Arnon [9] tarafından gerçekleştirilen, kablosuz algılayıcı ağlar kullanılarak görüş çizgisiz (NLOS – Non Line of Sight) optik iletişim çalışmasıdır.

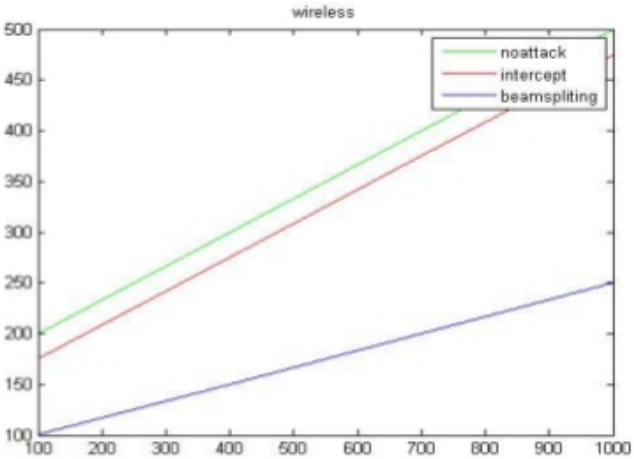
4. UYGULAMA SONUCU

Uygulamanın sonuçlarına bakıldığında, anahtar uzunluğu ile hata karşılaştırması deneylerinde kullanılan farklı değerler için üç ölçüm kriteri kullanılmıştır. Şekil 4 ve 5'te farklı ağ ortamları için grafiklerin karşılaştırması görülmektedir. Kablosuz ortamdan elde edilen fraksiyonun kablolu olanla karşılaştırıldığında daha düşük olduğu görülmektedir. Bunun sebebi sadece kablosuz ortamların saldırıya maruz olması değil, aynı zamanda kablolu ortamla karşılaştırıldıklarında çok daha gürültülü olmalarıdır.



Şekil 4: Anahtar Uzunluğu – Hata Oranı Karşılaştırması

Her iki şekil de, herhangi bir saldırı olmamasına rağmen, Barış'ın Ayşe tarafından gönderilen bit uzunluğunun tamamını alamadığını göstermektedir. Bu durum, kuantum kanalının bizzat kendisinin, iletim sırasında kanalı kısıtlayarak bitleri üzerinde yarattığı küçük bir miktar etkiden kaynaklanmaktadır. Aynı şey önleme amaçlı saldırılarda da (intercept) geçerlidir. Önleme amaçlı saldırı sırasında Engin, rasgele üretilmiş yeni bir katarı Barış'a göndererek, bu katarın Ayşe tarafından üretildiğini düşünmesini sağlar. Bu durumda, Engin tarafından üretilen anahtarın Ayşe'nin anahtarı zannedilme olasılığı %50 iken, Ayşe ve Barış'ın, Engin'in varlığını farketme olasılıkları %25'dir.



Şekil 5: Anahtar Uzunluğu – Hata Oranı Karşılaştırması

Beam Splitting saldırılarında hata bitinin uzunluğu diğer iki saldırıya oranla daha düşüktür çünkü bu saldırıda Ayşe tarafından gönderilen rasgele bir sayı Engin tarafından yakalanır. Bu sayede Ayşe ve Barış, hata düzenleme sürecinde çok daha fazla hata yakalayabilir.

Kablolu ve kablosuz uygulamada, Ayşe ve Barış arasındaki iletişimde ortaya çıkan gürültü miktarıyla bağlantılı olarak farklı değerlerde sonuç bitleri elde edilmiştir. Kablosuz ortamda, kablolu olana oranla daha fazla gürültü olduğundan, sonuç bitleri daha kısa çıkmıştır.

4. SONUÇ

Kablosuz ağların karşı karşıya oldukları çeşitli güvenlik riskleri bulunmaktadır. Kablosuz ağlardaki risklerin en göze çarpanı ve dikkat edilmesi gerekeni, iletişim teknolojisinin doğal ortamı olarak kabul edilmeye başlanan havada ilerleyen dalgaların (airwave) saldırılara açık olmasıdır. Bu sebepten kablosuz ağların güvenliği için günümüze kadar birçok çalışma yapıldı ve yapılmaya devam etmektedir. Bahsedilen bu sorunun çözüm çalışmalarından biri olarak, bu çalışmada 802.11 ağlarında anahtar dağıtımı için kuantum kriptografisi kullanımının anahatları çizildi. Kuantum kriptografisinin oluşturulmuş anahtar değişimi yöntemine göre avantajı, veri iletişiminin, bilinen bazı matematiksel problemlerle ilgili varsayımlarda bulunmak zorunda kalmadan, fiziksel olarak çok güçlü olarak algılanan bir güvenliği olduğunun kanıtlanmış olmasıdır. Bu çalışmada, KAD'nin koşulsuz güvenlik önlemleriyle IEEE 802.11 kablosuz ağlarının ortak çalışmasının genel hatları çizilmiştir. KAD, IEEE 802.11 gibi küçük çaplı kablosuz ağlarda güvenli veri iletişimi sunma konusunda daha iyi sonuçlar verir. Kuantum iletişimi için MIMO teknolojisindeki son gelişmeler donanımlardaki LOS kısıtını ortadan kaldırmaya başlamıştır. Şu ana kadar ki çalışmalar, mevcut 802.11 ekipmanını kuantum iletişimi yapacak şekilde genişletmeyi tam anlamıyla başaramasa da, bu çalışmanın geleceğin kablosuz ağlarında güvenli iletişim gelişmelerine katkı sağlayacağı değerlendirilmektedir.

KAYNAKLAR

[1] Xu Huang, Shirantha Wijesekera ve Dharmendra Sharma, "Implementation of Quantum Key Distribution in Wi-Fi (IEEE 802.11) Wireless Networks," Konferans Tutanağı: The 10th international Conference on Advanced Communication Technology, Şub 17- 20,2008 Phenonix Park, Korea. ISSN 1738-9445 ,ISBN 978-89-5519-135-6, cilt.II, sf. 865.

[2] ANSI/IEEE 802.11 , 1999 Sürümü (R2003),kısım 1.1: Wireless LAN Medium Access Control (MAC) and Physical Layer(PHY)Specifications.

[3] IEEE Std 802.11i,IEEE Standard for Information Technology – telecommunication and information exchange between systems-local and metropolitan area networks-Specific Requirements kısım 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, Amendment 6: Medium Access Control(MAC) Security Enhancements, 2004.

[4] IEEE802.1X,2004, IEEE Standard for Local and metropolitan area networks, Port-Based Network Access Control.

[5] Changhua He, John C Mitchell, Analysis of the 802.11i 4-way Handshake.

[6] Floriano De Rango, Dionogi Lentini ,Salvatore Marano, Static and Dyanmic 4-way Handshake Solutions to Avoid Denial of Service Attack in Wi-FI Protected Access and IEEE802.11i, Haz 2006.

[7] Bennett, C. H. and Brassard, G., "Quantum Cryptography: Public – Key distribution and coin tossing", Konferans Tutanağı: IEEE International Conference on Computers,Systems and Signal Processing, Bangalore India, December 1984, sf. 175-179.

[8] Changhua He, John C.Mitchell, Security Analysis and Improvements for IEEE802.11i.

[9] Debbie Kedar, Shiliomi Arnon, Non-line-of-sight optical wireless sensor network operating in multiscattering channel, 2006.

[10] Debbie Kedar, Shilomi Arnon, Quantum Key Distribution by a Free space MIMO System, May 2006.

[11] Bob O'Hara, A1 Petrick, IEEE 802.11 Handbook, A Designers's companion, 2005.

[12] D. Whiting, R. Housely, N.Ferguson, Request for Comments: 3610, Counter with CBC-MAC (CCM), Eyl 2003.

[13] B. Aboba, L.Blunk, J.Carlson, H.Levkowetz, RFC-3748, Extensible Authentication Protocol (EAP), 2004.

[14] Matthias Scholz, Quantum Key Distribution via BB*4, An Advanced Lab Experiment, Ağu 2005.

[15] Paul J.Edwards, Canberra Üniversitesi - Quantum Crypto-Key Telecommunications Link, Advanced Telecommunications and Electronics Research Centre, http://www.ips.gov.au/IPSHosted/NCRS/wars/wars2002/pro ceedings/ invited/ print/Edwards.pdf.

[16] ChangHua He, John C. Mitchell, 1 message Attack on the 4-way Handshake, May 2004.

[17] İnternet:http://www.computerworld.com/ security topics/security/story/ 0,10801,96111,00.html , Quantum cryptography gets pratical.

[18] Dagmar Bruβ, Optimal Eavesdropping in Quantum Cryptography with six States, Physical Review Letters, 81.3018, Eki 1998.

[19] M.s Goodman, P.Toliver, R.J.Runser, T.E. Chapuran, J.Jackel, R.J.Huges, C.G. Peterson, K.McCabe, J.E.Nordholt, K.Tyagi, P.Hisket , S.McNown, N.Nweke, J.T Blake, L.Mercer, H.Dardy, Quantum Cryptography for Optical Networks: A Systems Perspective.

[20] C.H.Bennett, Fiz.GG.Kağıdı: 68, 3121 (1992).

[21] Valerio Scarani,Antonio Acin, Gregoire Ribordy and Nicolas Gisin, Quantum Cryptography protocols Robust against Photon Number Splitting Attacks .

[22] Valerio Scarani,Antonio Acin,Gregoire Ribordy and Nicolas Gisin, Quantum Cryptography protocols Robust against Photon Number Splitting Attacks for Weak laser Pulse Implementations, Fiz.GG.Kağıdı: Cilt 92, 057901, 2004.

[23] Gilles Brassard, Norbert Lűtkeenhaus, Tal Mor, Barry C.Sanders, Limitations on Praticals Quantum Cryptogrphy, Şub 2000.

[24] Tom Kargiannis, Les Owens, Wireless Network Security, 802.11, Bluetooth and Handheld Devices, NIST, Özel Yayım 800-48, Kas 2002.

[25] Tobias Schmitt-Manderbach, Henning Weier, Martin Fűrst, Rupert Ursin, Felix Tiefenbacher, Thomas Scheidl, Josep Perigues, Zoran Sodnik, Christian Kurtsiefer, John G.Rarity, Anton Zeilinger Harald, Weinfurter , Experimental Demonstration of Free-space Decoy- State Quantum Key Distribution of Free-space Decoy-State Quantum Key Distibution over 144km, Phys.Rev.Lett . 8,01054, Oca 2007.

[26] İnternet: http://www.secoqc.net/, SECOQC, Development of a Global Network for Secure Communication based on Quantum Cryptography.

[27] İnternet: http://www.technologynewsdaily.com/node/8985,http://www.idqua ntique.com/, id Quantique, Quantum Cryptography.

[28] New Scientist, Quantum ATM rules out fraudulent web purchases,10 Kas 2007.