OPTİK AĞLARDA KUANTUM KRİPTOGRAFİ KULLANARAK GÜVENLİ İLETİŞİM

Mustafa TOYRAN[1]

[1]TÜBİTAK - UEKAE
P.K. 74, 41470, Gebze, KOCAELİ

[1]e-posta: mtoyran@uekae.tubitak.gov.tr

Anahtar sözcükler: Optik İletişim, Kuantum Kriptografi, İletişim Güvenliği

ÖZET

Bu bildiride optik iletişim ve güvenliği incelenecek, kuantum kriptografi kullanımına dayanan güvenli bir optik iletişim yöntemi ve analizleri sunulacaktır. Sunulan yöntemde kriptografik gizli anahtarlar taraflar arasında kuantum kriptografi kullanılarak dağıtılmaktadır. Kuantum kriptografi, sadece optik hatlar üzerinde uygulanabilen güvenli bir kriptografik gizli anahtar dağıtım ve iletişim yöntemidir. Klasik yöntemlerden farklı olarak anahtar dağıtımı sırasında kullanılan optik iletişim hattının dinlenip dinlenmediği de açığa çıkarılabilmektedir. Böylece anahtarlar bu teknikte diğer yöntemlere göre daha güvenli olarak dağıtılmış olmaktadır. Mesajlar daha sonra güvenle taşınan bu anahtarlarla gönderici tarafta şifrelenir ve alıcı tarafta tekrar çözülür. Böylece klasik yöntemlerle sunulandan daha güvenli bir iletişim ortamı da sağlanmış olur.

1. GİRİŞ

Işıkla iletişim insanlar tarafından çok eski zamanlardan beri kullanılmaktadır. Modern optik iletişim sistemleri öncesinde insanlar ateş yakarak, işaret fişekleri ve özellikle gemilerde ve deniz iletişiminde fenerler kullanarak uzak mesafelerle hızlı ve kolay iletişim ihtiyaçlarını gidermeye çalışmışlardır.

Milattan önce 525 ile 456 yılları arasında yaşayan Yunanlı trajedi yazarı Aeschylus, *Oresteia* isimli dramasında Troy'un düşüşü haberinin aralarında kuş uçuşu ile 400 km mesafe olan Küçük Asya'dan Argos'a (bugünkü Yunanistan) bir dizi işaret ışıkları kullanılarak nasıl gönderildiğini anlatır. Bu yöntem ışık kullanıldığı için hızlı olmasının yanında mesajın aynı anda birden fazla alıcıya ulaştırılması avantajına da sahiptir. 1790 ile 1794 yılları arasında Fransız Claude Chappe de bir dizi flama kullanımına dayanan bir optik telgraf sistemi kurmuştu. Bu sistemde istasyonlar birbirinden 10-20 km, dürbünle görüş mesafesi kadar, arayla konumlanmaktaydı ve dakikada 3-4 karakter taşınabiliyordu. Ancak, Chappe'nin optik telgrafı kötü hava koşullarından olumsuz yönde etkilenmesi ve gece de kullanılamaması nedeniyle 19. yüzyılın sonlarına doğru yerini elektrikli telgrafa bırakmıştır [1].

Haberleşmede ışık kullanımı sahip olduğu avantajları nedeniyle günümüzün de en tercih edilen iletişim yöntemlerinden biridir. Kullanımının her geçen gün daha fazla yaygınlaşması, diğer iletişim tekniklerinde olduğu gibi, bu iletişim yönteminin güvenliğini de önemli bir konu haline getirmektedir.

Bildirinin sonraki kısımlarında sırasıyla şu konular ele alınmaktadır: Bölüm 2'de optik iletişimden ve güvenliğinden bahsedilmektedir. Bölüm 3'te kuantum kriptografi kullanımına dayanan güvenli optik iletişim yöntemine ve analizlerine değinilmektedir. Bölüm 4'te ve Bölüm 5'te ise sırasıyla tartışma ve sonuç bölümleri yer almaktadır.

2. OPTİK İLETİŞİM

Optik iletişim, haberleşme için ışık kullanılan iletişim tekniğidir. İletişim ortamı fiber optik kablo olup mesajlar taraflar arasında optik fiberler üzerinden ışık darbeleri ile gönderilir ve alınır.

Işığın mesaj göndermek için kullanımı uzun bir geçmişe sahip olmasına rağmen, 1880 yılında Alexander Graham Bell'in güneş ışığının yoğunluğunu modüle ederek birkaç yüz metre öteye mesaj gönderebildiği fototelefonu (photophone) yapmasıyla teknolojide bir devrim yaşanmıştır. 1880 yılının sonlarından 1960 yılının başlarına kadar düşük kapasiteli ve kısa mesafeli optik iletişim kullanılagelmiştir.

1960'larda lazerin keşfi, 1970'lerde düşük kayıplı optik fiberin geliştirilmesi, 1980'lerde uzun ömürlü

yarıiletken lazer diyodların kullanımına başlanması ve 1990'larda pratik optik kuvvetlendiricilerin geliştirilmesi optik iletişimde yeni bir dönemin başlamasına neden olmuştur [2].

Bugün gelinen noktada modern optik fiber sistemleri ile hızlı ve okyanusları aşan/kıtalararası mesafelerde iletişim gerçekleştirmek mümkündür. Benzer şekilde serbest-uzay iletişim sistemleri de uydular arasında yüksek data hızlı veri iletişimi olanağı sağlamaktadır. Optik iletişim, bu mikrodalga ve/veya kablosuz teknolojilerle birlikte, geniş çaplı bir bağlanabilirlikle, yüksek kapasiteli ağların kurulmasına olanak tanımaktadır.

Optik iletişim için en çok kullanılan dalgaboyları 0.83 ile 1.55 mikron arasındadır. 1 mikronluk bir dalgaboyu 300 THz'lik (300,000 GHz) bir frekansa karşı düşmektedir. Bu değer geleneksel radyo, mikrodalga veya milimetre-dalga iletişim sistemlerindeki frekanslara göre oldukça yüksek bir değer olup, optik iletişimin bant genişliğinin çok daha yüksek olması anlamına gelmektedir.

2.1 AVANTAJLARI

Optik iletişimin geleneksel bakır kablolu ve/veya kablosuz iletişime göre birçok avantajları vardır. Bunlardan bazıları aşağıdaki gibidir [3]:

- Fiber optik kablolar bakırlara göre daha ince ve daha hafiftirler. Bu nedenle daha az yer kaplarlar ve idareleri daha kolaydır.
- Bant genişliği daha yüksektir. Aynı anda çok daha büyük miktarlarda veri taşınabilir. Modern optik iletişim sistemlerinde erişilebilir bant genişliği 50,000 Gbps (50 Tbps) ve üzeridir.
- Kayıplar daha az olup veriler daha hızlı bir şekilde daha uzak mesafelere taşınabilir. Modern optik iletişim sistemlerinde iletim hızı 1 Gbps ve üzeridir. Tek bir fiber üzerinde bu değer 100 Gbps'ye kadar çıkabilmektedir. Fiberde ışık sinyalleri daha az zayıflamaya uğradığından tekrarlayıcılara gerek olmadan uzun mesafeli bağlantılar gerçekleştirilebilir. Optik fiberde yaklaşık olarak 50 km'de bir tekrarlayıcıya gerek olmaktadır.
- Fiber kablolar elektriksel parazitlerden ve olumsuz hava koşullarından hiç etkilenmezler. Bu nedenle sinyaller bozulmadan, daha kaliteli taşınır. Modern optik iletişim sistemlerinde hata hızı neredeyse 0'dır.
- Fiber kablolara bağlanıp bilgi çalmak, imkansız olmasa da, çok daha zordur. Bu nedenle optik fiber iletişimi daha güvenlidir.

2.2 GÜVENLİĞİ

Verilen avantajlarından dolayı optik iletişim günümüzün en tercih edilen iletişim yöntemlerinden biri haline gelmiş durumdadır. Diğer iletişim tekniklerinde olduğu gibi optik iletişimde de taşınan verilerin güvenliği önemlidir ve gerekli önlemlerin alınması gerekir.

İletişim sistemlerinde karşılaşılabilecek başlıca bilgi güvenlik ihlalleri şu şekilde özetlenebilir:

- İletim hattına bağlanıp iletişim dinlenebilir.
- Taşınan bilgilerin içerikleri değiştirilebilir.
- Hatta girilip sahte mesajlar yollanarak gönderici ve alıcı aldatılabilir.

Günümüzde, bahsedilen bilgi güvenlik ihlallerinin önüne geçmek için kullanılan başlıca araç kriptografidir. Modern kriptografi bilgilerin gerçek alıcısı dışındakilerin anlayamayacağı şekilde içeriğinin gizlenmesi, değiştirilip değiştirilmediğinin ve gerçek göndericisinin doğrulanması için araçlar sunmaktadır.

Ancak, modern kriptosistemlerde gizli anahtarların varlığına güvenilmektedir. Güvenlik bu gizli anahtarların gizliliğine ve dağıtımlarının güvenliğine bağlıdır. En büyük problem ise anahtarların gizliliğinin hiçbir zaman garanti edilememesidir. Bilinen bütün klasik anahtar dağıtım yöntemlerinin çeşitli zayıflıkları bulunmaktadır. Ayrıca, bu teknikler kullanılan iletişim ortamının güvenli olup olmadığı hakkında da herhangi bir bilgi veremezler.

Dolayısıyla, bahsedilen anahtar dağıtım ve iletişim sorunlarının olmadığı bir iletişim tekniğine ihtiyaç bulunmaktadır.

3. KUANTUM KRİPTOGRAFİ İLE GÜVENLİ OPTİK İLETİŞİM

Bu bölümde kuantum kriptografi kullanımına dayanan güvenli bir optik iletişim yöntemi ve analizleri sunulmaktadır. Sunulan yöntemde:

- Gizli anahtarlar taraflar arasında kuantum kriptografi kullanılarak dağıtılmaktadır.
- Anahtar dağıtımı esnasında iletişim hattının dinlenip dinlenmediği de belirlenebilmektedir.

Kuantum kriptografi, iletişimin optik kanallar üzerinden fotonlar kullanılarak gerçekleştirildiği kriptografik bir gizli anahtar dağıtım yöntemidir. İletişim esnasında kullanılan optik hatta bir müdahale olup olmadığını da açığa çıkarabilmektedir.

İlk kuantum kriptografi protokolü 1984 yılında Charles Bennett ve Gilles Brassard tarafından keşfedilmiştir [4]. Bu protokol, BB84 protokolü olarak da bilinmektedir [5,6,7]. Bu çalışmada, BB84 protokolünün tanıtımı ve analizleri yapılmaktadır.

3.1 ANAHTAR DAĞITIMI

Foton, ışığı oluşturan taneciklerden herbirine verilen addır. Fotonların bir biti kodlamada kullanılabilecek

çeşitli özellikleri bulunmaktadır: frekans, faz, polarizasyon, vb.. Kuantum kriptografide çoğunlukla fotonun polarizasyon özelliğinden yararlanılır.

Kuantum anahtar dağıtım ve iletişim yöntemi özetle şu şekilde çalışmaktadır:

+	--------> |	–	Foton
X	--------> /	\	polarizasyonları
	1	0	Bit eşdeğeri

Şekil 1. Bitleri foton polarizasyonları ile kodlama kuralları

Protokolü koşturmadan önce göndericinin ve alıcının Şekil 1'deki gibi bir kodlama kuralı üzerinde anlaşmış olması gerekir.

Göndericinin bitleri	**0**	1	0	**1**	0	0	**0**	**1**	**0**	**1**
Göndericinin polarizasyon tabanları	+	+	X	+	+	+	+	X	+	X
Gönderilen fotonlar	–	|	\	|	–	–	–	/	–	/

Alınan fotonlar	–	|	\	|	–	–	–	/	–	/
Alıcının polarizasyon tabanları	+	X	+	+	X	X	+	X	+	X
Alıcının bitleri	**0**	1	0	**1**	0	0	**0**	**1**	**0**	**1**

Gizli Anahtar: 0 1 0 1 0 1

Şekil 2. Fotonlarla anahtar dağıtımı

- Gönderici öncelikle rasgele bir bit dizisi seçer. Alıcının seçilen bu bit dizisinden haberi yoktur.
- Gönderici herbir biti için rasgele bir polarizasyon tabanı (+ veya X) belirler, bitini bu tabanda Şekil 1 uyarınca uygun (|, –, / veya \ ) polarize edilmiş fotonla kodlar ve fotonu alıcıya gönderir.
- Alıcı gelen herbir fotonun polarizasyonunu ölçer. Ancak göndericinin fotonu polarize ederken hangi polarizasyon tabanını kullandığını bilmemektedir. Bu nedenle ölçümü sırasında her bir foton için kullanacağı polarizasyon tabanını rasgele seçer. Sonuçta, alıcı gelen fotonları rasgele ölçer ve o da Şekil 1 uyarınca bir bit dizisi elde eder.
- Gönderici ve alıcı sadece kullandıkları polarizasyon tabanlarını kimlik kanıtlamalı bir kanal üzerinden, örneğin telefonla, birbirlerine açıklar. Aynı polarizasyon tabanlarını kullandıkları durumlar için gönderilen ve alınan bitler kesinlikle aynı olacaktır. Bu ortak, ama gizli, bitler *anahtar* olarak kullanılırlar. Şekil 2'de taraflar 6 bitlik 010101 gizli anahtarı üzerinde anlaşmıştır.

Protokol sonunda mesaj belirlenen anahtarla gönderici tarafta şifrelenir ve alıcı tarafta tekrar çözülür.

3.2 MÜDAHALENİN ANLAŞILMASI

Kuantum kriptografide aynı polarizasyon tabanının kullanıldığı bir durum için gönderilen ve alınan bir bitin farklı çıkması hattı dinleyen şüphelilerin varlığına işarettir. Bu özellik kullanılarak kullanılan iletişim hattının güvenliğini doğrulamak, hatta şüpheli bir müdahale olup olmadığını açığa çıkarmak da mümkündür.

Arada birinin olması durumunda göndericinin gönderdiği fotonları önce saldırgan alır ve yaptığı ölçümler neticesinde o da bir bit dizisi belirler. Fotonların kuantum doğasına göre saldırgan fotonları kopyalayamadığından (kopyalanamazlık ilkesi) onları yeniden oluşturur ve alıcıya bu yeni fotonları gönderir (bkz. Şekil 3).

Arada birinin olup olmadığını belirlemek için gönderici ile alıcı protokolün son aşamasında önce bitlerden bir alt küme için hem polarizasyon tabanlarını hem de bitlerin değerlerini karşılaştırırlar (saldırganı belirleme testi). Polarizasyon tabanında anlaştıkları bir durum için gönderilen ve alınan bitte de kesinlikle uyuşma olmalıdır.

Göndericinin bitleri	**1**	0	1	0	0	**0**	0	0	**0**	**0**
Göndericinin polarizasyon tabanları	+	+	+	X	X	+	X	X	X	X
Gönderilen fotonlar	|	–	|	\	\	–	\	\	\	\

Alınan fotonlar	|	–	|	\	\	–	\	\	\	\
Saldırganın polarizasyon tabanları	+	X	X	+	X	X	X	+	X	X
Saldırganın bitleri	1	0	0	1	0	1	0	1	0	0

Saldırganın bitleri	1	0	0	1	0	1	0	1	0	0
Saldırganın polarizasyon tabanları	+	X	X	+	X	X	X	+	X	X
Gönderilen fotonlar	|	\	\	|	\	/	\	|	\	\

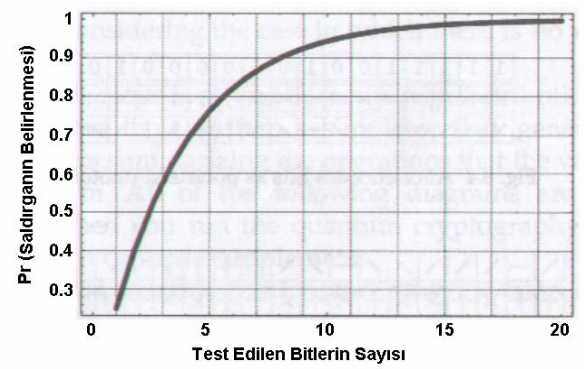
Alınan fotonlar	|	\	\	|	\	/	\	|	\	\
Alıcının polarizasyon tabanları	X	+	+	X	X	+	X	X	+	X
Alıcının bitleri	**1**	1	0	0	0	**1**	0	1	**0**	**0**

Şekil 3. Arada bir saldırganın bulunması durumunda anahtar dağıtımı ve saldırganın tespiti

Şekil 3'te görüldüğü gibi, test edilen koyu renkli bitlerden ikincisinde (soldan sağa doğru 6. bit) saldırgandan kaynaklanan bir hata görülmektedir. Bu hata arada hattı dinleyen birinin bulunduğunu açığa vurmaktadır.

Ne kadar fazla sayıda bit test edilirse araya girerek hattı dinleyen biri(leri)nin varlığını saptama olasılığı da o kadar fazla olacaktır. Gönderici ve alıcı tarafından test edilen N bit için bu testin araya giren

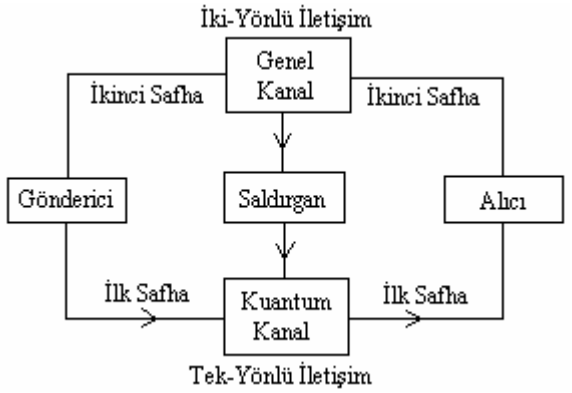
birilerinin varlığını açığa çıkarma olasılığı 1-(3/4)^N'dir [5,6,7]. Bu fonksiyonun grafiği Şekil 4'te verilmiştir.



Şekil 4. Test bitlerinin sayısına bağlı olarak saldırganın belirlenmesi olasılığı [7]

Sonuçta, hattı dinleyen birileri varsa gönderici ile alıcı görüşmelerini sonlandırmaya karar verirler.

Yapılan test sonucu hattın dinlendiği saptanamamışsa anahtar test bitleri dışındaki bitler arasından ilk yöntemde anlatıldığı gibi belirlenir. Ve mesaj bu anahtar kullanılarak göndericide şifrelenir ve alıcıda tekrar çözülür.



Şekil 5. Kuantum kriptografi iletişim sistemi [5]

3.3 GERÇEKLEME

Kuantum kriptografi iletişim sistemi Şekil 5'te görüldüğü gibi birbirinden farklı iki kanaldan oluşmaktadır: foton iletişimin gerçekleştirildiği ilk safha için kullanılan bir kuantum kanal ile anahtarı belirlemede ve saldırganın tespitinde kullanılan ikinci safha için bir klasik kanal.

Klasik kanal olarak, bilinen telefon hattı, GSM, İnternet ve benzeri kablolu/kablosuz herkese açık iletişim ortamları kullanılabilir. Klasik kanal üzerindeki iletişimde tarafların birbirlerinin kimliklerinden emin olmaları önemlidir.

Kuantum kanal olarak ise fotonları iletme özelliğine sahip herhangi bir kanal, örneğin optik fiber, kullanılması gerekir. Klasik kanalda olduğu gibi kuantum kanalın da gizli olması gerekmez.

Kuantum kanal üzerinden yapılan foton iletişimi için göndericide foton kaynağı ve foton polarize edici; alıcıda ise foton dedektörü ve foton polarizasyon ölçücü gibi bileşenlere ihtiyaç olmaktadır.

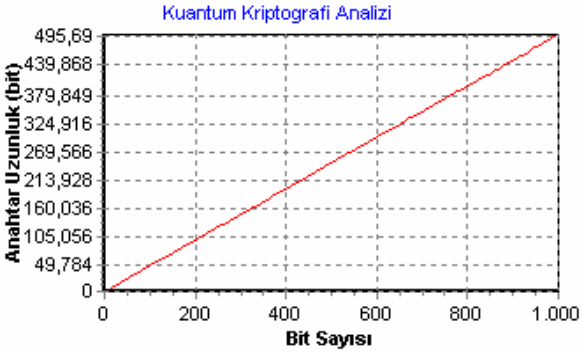
Protokolde gereken rasgele değerler için de güvenilir bir rasgele sayı üretecine ihtiyaç vardır. Bu değerlerin rasgele olması protokolün güvenliği açısından çok önemlidir.

Çeşitli kuantum kriptografi gerçeklemeleri için [8-12] incelenebilir.

Bu çalışmada kuantum kriptografinin Windows 2000 işletim sistemi yüklü klasik bir bilgisayar üzerinde C programlama dili kullanılarak benzetimi yapılmış ve aşağıdaki analizler gerçekleştirilmiştir.

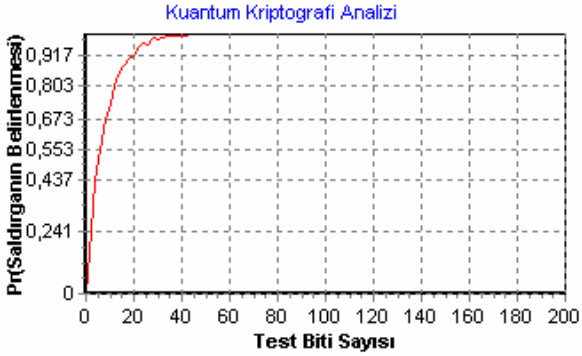
3.4 ANALİZLER

Aşağıda verilen bilgisayar analizleri en iyi, gürültüsüz, durumlar için olup dağıtılan anahtarların uzunlukları ve saldırganın tespit edilmesi durumları üzerinedir.



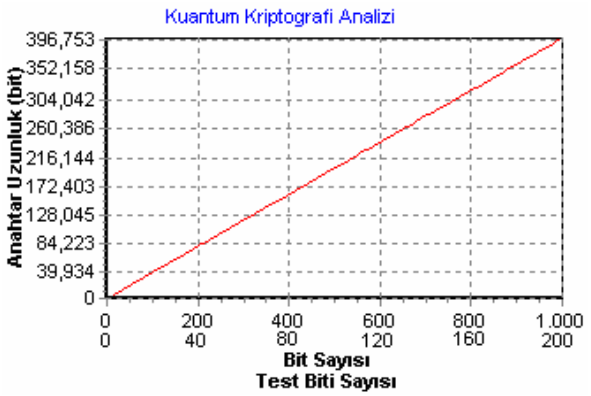
Şekil 6. Elde edilen anahtar uzunlukları

- **Anahtar Uzunlukları:** Bu analiz için Şekil 2'de verilen protokolde başlangıç bit uzunluğu 10'dan başlatılarak 10'ar artımla 1000'e kadar değiştirilmiş ve her bir giriş için toplam 1000 adet deneme yapılmıştır. Denemeler sonucu her bir giriş için elde edilen toplam anahtar uzunluğu toplam deneme sayısına (1000'e) bölünerek ortalama anahtar uzunluğu bulunmuş ve çizdirilmiştir. Analiz sonuçlarına göre, Şekil 6'dan da görüldüğü gibi, protokol sonunda elde edilen anahtarların uzunlukları yaklaşık olarak protokol başında seçilen rasgele bit dizisinin yarısıdır.



Şekil 7. Saldırganın belirlenme olasılığı

- **Saldırganın Belirlenmesi:** Bu analiz için Şekil 3'te verilen protokolde başlangıç bit dizisi tüm denemeler için sabit ve 1000 olarak ayarlanmıştır. Saldırganı belirlemekte kullanılacak test bitlerinin sayısı ise 2'den başlatılarak 2'şer artımla 200'e kadar değiştirilmiş ve her bir durum için toplam 1000 deneme yapılmıştır. Elde edilen sonuçlar Şekil 7'de görüldüğü gibidir. Buna göre yaklaşık olarak 20 tane test bitinden sonra saldırganın yakalanma olasılığı neredeyse 1 olmaktadır.



Şekil 8. Test bitleri kullanılması durumunda elde edilen anahtarların uzunlukları

- **Saldırganın Olmaması:** Şekil 3'te verilen protokolde bu kez arada saldırgan olmasın. Bu durumda taraflar ortak bir gizli anahtar üzerinde anlaşacaktır. Test bitlerinin sayısı 2'den başlayıp 2'şer artımla 200'e kadar değişirken, başlangıç bit uzunluğu bu kez 10'dan başlatılarak 10'ar artımla 1000'e kadar değişsin. Elde edilen anahtarların uzunlukları Şekil 8'de görüldüğü gibidir. Bazı bitlerin test biti olarak kullanılmasından dolayı elde edilen anahtarlar Şekil 6'dakilere göre daha kısa olmaktadır.

Benzetim sonuçlarından da görüldüğü gibi, kuantum kriptografi kullanılarak kriptografik gizli anahtarların dağıtımı gerçekleştirilebilmekte ve bu esnada, klasik yöntemlerden farklı olarak, kullanılan iletişim hattının dinlenip dinlenmediği de açığa çıkarılabilmektedir.

4. TARTIŞMA

Kuantum kriptografi optik bir iletişim tekniğidir. Dolayısıyla, sunulan yöntemin uygulanabilmesi için optik bir iletişim altyapısına ihtiyaç vardır.

Ayrıca, kuantum kriptografi taraflar arasında uçtan uca bir optik bağlantı ve fotonlarla çalışmayı gerektirmektedir. Bu durum çok uzak mesafeler için kuantum kriptografi kullanımını zorlaştırır. Uçtan uca optik hat üzerinde fotonların polarizasyonunu etkileyebilecek bükülme, ezilme, tekrarlayıcı, bağlantı noktaları vb. de olmaması gerekir. Foton gibi kuantum sistemler hatalara karşı çok duyarlı olup, en küçük etkiden çok fazla rahatsız olur. Böyle sistemlerle çalışmanın bir diğer zorluğu da maliyetlerinin henüz çok yüksek olmasıdır. Bunlar kuantum kriptografi kullanımını kısıtlayan başlıca etkenlerdir.

Gelecekte gerçek kuantum sistemleri inşa edildiğinde kuantum kriptografiden de en iyi verim elde edilebilecektir.

5. SONUÇLAR

Optik iletişim tek bir fiberde Tbps'yi aşan yoğunlukta trafik taşıyabilme kapasitesiyle günümüzün tercih edilen iletişim yöntemlerinden biri haline gelmiş durumdadır. Diğer iletişim tekniklerinde olduğu gibi optik iletişimde de taşınan bu büyük miktardaki bilgilerin güvenliğinin sağlanması önemlidir.

Günümüzde bilgi güvenliğini sağlamak üzere kullanılan başlıca araç bilgiyi şifrelemedir. Modern şifreleme sistemlerinde güvenlik gizli anahtarların gizliliğine ve dağıtımının güvenliğine bağlıdır. Ancak en büyük problem de bu gizli anahtarların gizliliğinin hiçbir zaman garanti edilememesidir. Bilinen bütün klasik anahtar dağıtım yöntemlerinin çeşitli zayıflıkları bulunmaktadır. Ayrıca, bu teknikler kullanılan iletişim ortamının güvenliği ve taşınan bilgilerin kopyalanıp kopyalanmadığı hakkında da bir bilgi veremezler.

Kuantum kriptografi kullanıldığında bu sorunlar giderilebilmektedir. Bu teknikte anahtarlar taraflar arasında fotonlar kullanılarak güvenli bir şekilde dağıtılır. Üstelik, kullanılan iletişim hattının dinlenip dinlenmediği de açığa çıkarılabilmektedir. Mesajlar daha sonra güvenle taşınan bu anahtarlarla şifrelendiğinde mevcut yöntemlere göre daha güvenli bir iletişim ortamı da sağlanmış olur.

KAYNAKLAR

[1] Einarsson G., 1996. "Principles of Lightwave Communications", John Wiley & Sons Ltd.

[2] Alexander B. A., 1997. "Optical Communication Receiver Design", The Society of Photo-Optical Instrumentation Engineers.

[3] Tanenbaum A. S., 2003. "Computer Networks Fourth Edition", Prentice Hall PTR.

[4] C. H. Bennet and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing", Proc. Int'l Conf. Computers, Systems & Signal Processing, CS Press, 1984, pp. 175–179.

[5] S. J. Lomonaco, "A Quick Glance at Quantum Cryptography", http://www.csee.umbc.edu/~lomonaco, 1998.

[6] Gisin N., Ribordy G., Tittel W. and Zbinden H., "Quantum cryptography", Rev. Mod. Phys., vol. 74, 2002, pp. 145–195.

[7] Williams C. P., Clearwater S. H., 1998. "Explorations in QUANTUM COMPUTING", Springer-Verlag NewYork, Inc. TELOS.

[8] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, J. Smolin, "Experimental Quantum Cryptography", Journal of Cryptology, Vol. 5, 1992, pp. 3-28.

[9] V. Sochor, "Fiber optic quantum cryptography", Proc. SPIE Vol. 2799, pp. 185-187, Atomic and Quantum Optics: High-Precision Measurements, Anatoliy S. Chirkin; Sergei N. Bagayev; Eds, 05/1996.

[10] D. S. Bethune and W. P. Risk, "An autocompensating fiber-optic quantum cryptography system based on polarization splitting of light", IEEE J. Quant. Elect., 36, 1998, pp. 340-347.

[11] R. Alléaume, J.-F. Roch, D. Subacius, A. Zavriyev, and A. Trifonov, "Fiber-optics quantum cryptography with single photons", AIP Conference Proceedings 734, 2004, pp. 287-290.

[12] C. Gobby, Z. L. Yuan ve A. J. Shields, "Quantum key distribution over 122 km standard telecom fiber", Appl. Phys. Lett., 84, 2004, pp. 3762–3764.