T.C.

YILDIZ TEKNİK ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

OPTİK İLETİŞİM AĞLARINDA FİZİKSEL KATMAN GÜVENLİĞİ

Ali RÜVEYCAN

ARAŞTIRMA PROJESİ

Elektronik ve Haberleşme Mühendisliği Anabilim Dalı

Haberleşme Tezli Yüksek Lisans Programı

Araştırma Yöntemleri ve Bilimsel Etik Dersi

Öğretim Elemanı

Prof. Dr. Tülay YILDIRIM

İÇİNDEKİLER

1
GİRİŞ

Optik iletişim, optik lif boyunca ışık sinyalleri göndererek bilginin bir yerden başka bir yere iletilmesi metodudur. Işık, bilgi taşınması için yönlendirilmiş elektromanyetik taşıyıcı görevi görür.

Optik iletişimin avantajları olarak; çok büyük bant genişliği potansiyeli, küçük ebat ve hafiflik, elektriksel yalıtım, elektromanyetik girişim etkileşmesinin olmaması [13], sinyal emniyeti, düşük iletim kaybı, dayanım ve esneklik, düşük maliyet ve sistem güvenilirliği ile bakım kolaylığı sayılabilir.

Optik iletişimin başlıca kullanım alanları olarak; ses, veri ve video iletimi, telekomünikasyon, yerel alan şebekeleri, endüstriyel kontrol sistemleri, aviyonik sistemler, askeri komuta kontrol ve haberleşme sistemleri sayılabilir [21].

Son yıllarda sağladığı avantajlar dolayısıyla optik iletişim, veri iletimi için çekici bir sistem haline gelmiştir.

Optik ya da optik olmayan bir iletişim ağında fiziksel katman, verilerin kablo üzerinden gelen bilgiyi bit olarak (0 ve 1 olarak) iletilmesini sağlar. Verileri gönderen tarafta 1 ve 0'ı elektrik sinyallerine dönüştürürken, alıcı tarafta kablodan gelen bu sinyalleri 1 ve 0'a dönüştürür.

Fiziksel katman yani donanım katmanı OSI modeline göre ilk katmandır. Bu katmanda çalışan donanımlar: fiber optik kablolar, radyo sinyal gönderici alıcılar, konnektörler ve tüm anahtarlardır.

İnternet üzerinden değiş tokuş edilen veri miktarı son yıllarda katlanarak artmakta ve bu sebepten dolayı hassas veri miktarı da artmaktadır. Bu durumlar bilgi güvenliği ve katman güvenliği gibi konuları da öne çıkarmaktadır.

2
AMAÇ VE HEDEFLER

Yüksek bant genişliği, düşük güç tüketimi ve düşük iletim kaybı gibi özellikleri ile optik ağlar hızla büyüyen bant genişliği taleplerini karşılamak için en uygun çözüm olarak kabul edilmiştir.

Bununla birlikte ana optik ağ bileşenleri, ağ içindeki yeni güvenlik açıklarının eşlik ettiği bir dizi güvenlik sorunu ve güvenilirlik sorunu ortaya çıkarmıştır.

Telefon dinleme kodlaması, gizli anahtar üretimi (SKG), fiziksel klonlanamayan işlevleri (PUF) kullanarak kimlik doğrulama, yerelleştirme / RF parmak izi, fiziksel katmanı izleyen anormallik algılama (PHY) gibi geniş bir teknoloji yelpazesi toplu olarak fiziksel katman güvenliği (PLS) olarak adlandırılır [12].

Günümüzde güvenli iletişimi garanti eden en yaygın kullanılan teknik, büyük asal sayıları çarpmanın karmaşıklığından yararlanan gizli kriptografik anahtarlara dayanmaktadır. Bununla birlikte, kriptografik algoritmalar çeşitli zorluklarla karşı karşıyadır. İlk olarak, bilgisayarların paralel ağları, yüksek performanslı bilgisayarlar kullanarak sonlu bir süre içinde güvenli kabul edilen kodları kırdığından, beklenmedik teknolojik gelişmelere karşı savunmasızdırlar. İkincisi, kriptografik algoritmaların fiziksel uygulamalarını ele alan talepler geleneksel yarı iletken teknolojisinin kısıtlamalarının ötesine geçer. Üçüncüsü, dijital anahtarı çalan bir hırsız farkedilmeyebilir [1].

Bu dezavantajların üstesinden gelebilmek için, gizli anahtar üretimi için fiziksel parametreler ile fiziksel kriptografik yöntemlerin araştırmaları yapılmıştır.

Bir iletişim sisteminde legal alıcı ve verici (Alice ve Bob) ve illegal kulak misafiri (Eve) olduğu varsayıldığında iletişim sürecini kulak misafirinden koruma sürecinde 2 durum söz konusudur. Birincisi, Eve'in legal alıcı ve vericiler arasındaki gizli bir parametreyi veya kodu bilmediği saf bir varsayımdır. İkincisi ise sistem çalışırken Eve'in Alice ve Bob arasındaki tüm olası süreci bildiği zorlu varsayımdır.

Bu araştırma projesinde amacımız ve hedefimiz, optik ağlarda her iki durum için de fiziksel katman güvenliğini sağlamanın yollarını araştırmak, literatür taraması sonuçlarını paylaşmak ve fiziksel katman güvenliği için uygulanabilecek yöntemlere değinmektir.

3
ARAŞTIRMA SORULARI

Bu araştırma projesi kapsamında okuyucu aşağıdaki sorulara cevap bulacaktır.

1. Optik iletişim nedir?
2. Optik veya optik olmayan bir ağda fiziksel katmanın güvenliğinin önemi nedir?
3. Optik ağlarda fiziksel katman güvenliği için ne gibi yöntemler önerilmiştir?
4. Fiziksel katman güvenliği için uygulanan tekniklerin yetersiz kaldığı noktalar nelerdir?
5. Fiber optik ağlarda fiziksel katman güvenliğini ihlal eden saldırılar nasıl sınıflandırılır?
6. 6G ağlarda fiziksel katman güvenliği için neler hedeflenmektedir?
7. Optik kablosuz haberleşme için fiziksel katman güvenliği adına neler yapılmıştır?
8. Free Space optik iletişimde fiziksel katman güvenliğinin önemi nedir?
9. Bir fiziksel katmanda şifreleme ve şifre çözme adımları neyi ifade eder?
10. Optik ağlarda saldırılara karşı alınabilecek çözüm yöntemleri nelerdir?
11. Optik ağlarda fiziksel katman için gizli anahtar üretimi nedir?

4
HİPOTEZ

Elektronik haberleşme yoluyla değiş tokuş edilen veri miktarı son yıllarda katlanarak arttı. Bu durum akabinde hassas veri miktarını da aynı şekilde arttırmış ve bilgi güvenliği çok önemli bir hale gelmiştir. Günümüzde güvenli iletişimi garanti eden en yaygın kullanılan teknik, büyük asal sayıları çarpmanın karmaşıklığından yararlanan gizli kriptografik anahtarlara dayanmaktadır. Bununla birlikte, kriptografik algoritmalar çeşitli zorluklarla karşı karşıyadır. İlk olarak, bilgisayarların paralel ağları, yüksek performanslı bilgisayarlar kullanılarak sonlu bir süre içinde güvenli kabul edilen kodları kırdığından, beklenmedik teknolojik gelişmelere karşı savunmasızdır. İkincisi, kriptografik algoritmaların fiziksel uygulamalarını ele alan talepler geleneksel yarı iletken teknolojisinin kısıtlamalarının ötesine geçer. Üçüncüsü, dijital anahtarı çalan bir hırsız farkedilmeyebilir.

Hesaplamalı kriptografinin bu dezavantajlarının üstesinden gelinerek, gizli anahtar üretimi için fiziksel parametreler kullanılarak fiziksel kriptografik yöntemlerin araştırmaları yapılmıştır.

Genel olarak çalışmalarda, bir iletişimde kulak misafirinin legal alıcı ve verici arasındaki gizli bir parametreyi ve kodu bilmediği gibi saf varsayımlar yapılır.

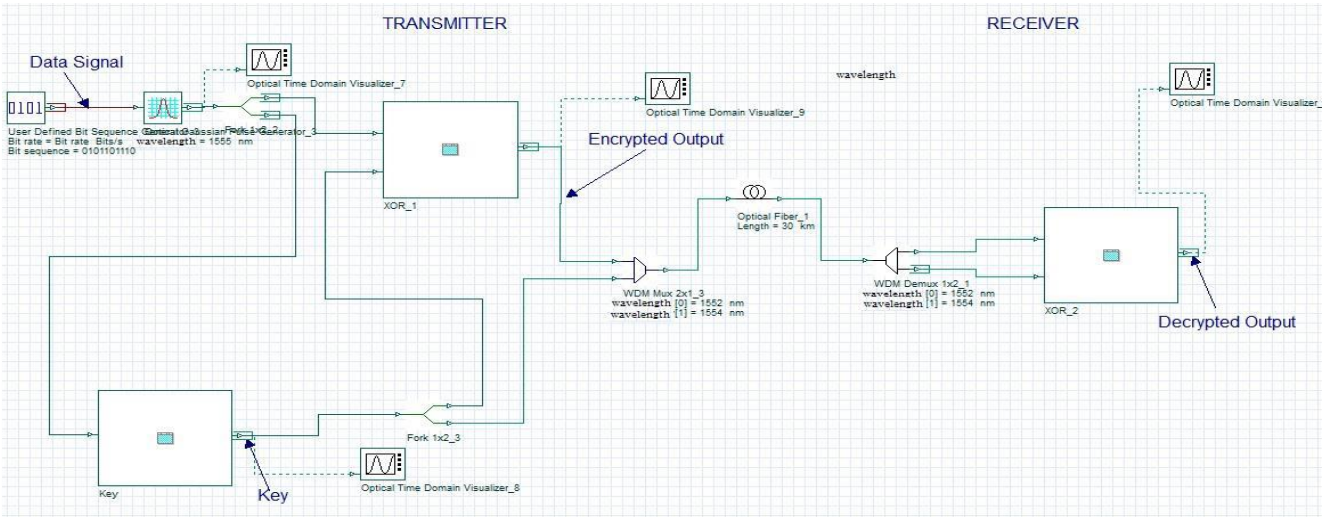
Bu çalışmada hipotez olarak ortaya atılan durum ise şudur: İllegal kulak misafirinin sistem çalışırken ve sisteme girmeye izni olmasına rağmen kalibrasyon sırasında legal alıcı ve verici arasındaki bilgi güvenliğinin özel bir fiziksel katman güvenliği (PLS) yöntemi ile yine de sağlanabiliyor olduğudur.

5
LİTERATÜR TARAMASI

5.1 1.Yöntem

Optik ağlarda fiziksel katman güvenliğini sağlamak için birçok yöntem sunulmuştur. İlk yöntem, SOA(Yarı iletken optik yükselteç)'da P-I-N fotodiyodunda ve XPM'de atış gürültüsü dalgalanmalarından üretilen sözde rasgele ikili dizi (PRBS) kullanılarak optik ağ güvenliğini geliştirmek için optik şifreleme ve şifre çözme yöntemidir [2].

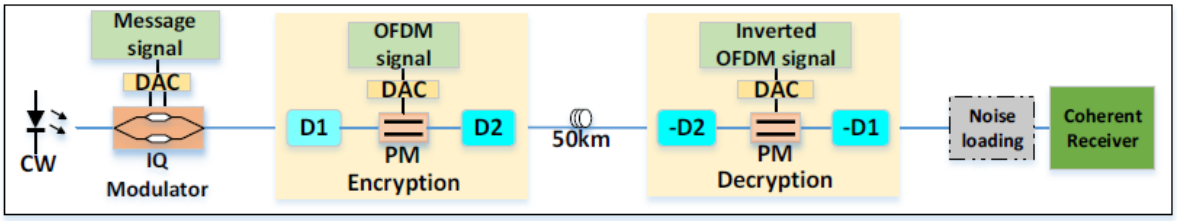
Bugün optik ağlar; optik amplifikatörler, optik çoklayıcılar gibi daha fazla optik bileşenle gelişti, böylece tek fiber veri hızını saniye başına Terabit sırasına göre iletebilir. Geleneksel ağda, depo ve ileri temel düğüm nedeniyle saldırılarda bir artış vardır. Bu nedenle fiberoptik ağ tercih edilen ağ olmuştur. Günümüz optik ağları, yüksek güçte sıkışma, fiziksel altyapı saldırıları, hizmet reddi, hizmet kesintisi, saldırıları dinleme ve trafik analizi için kullanılabilecek çeşitli saldırı biçimlerine karşı oldukça savunmasızdır. Örneğin: bir fiberi hafifçe bükerek ve ışığı yayarak veya içine ışığı bağlayarak belirli bir dalga boyunda sinyalleri vurmak veya sıkıştırmak oldukça kolaydır. Şifreleme ve şifre çözme, dünyanın en hassas verilerinin çoğunu güvence altına almak için hükümetler ve savunma güçleri tarafından yıllarca kullanıldı. Şifreleme, özellikle yetkisiz kullanıcılardan gelen orijinal bilgileri gizlemek veya kilitlemek için bir şifreleme algoritması kullanılarak orijinal mesajı tanınmayan veya kodlanmış bir forma dönüştürme işlemidir. Şekil-1 'de yukarıda bahsedilen yöntemin şeması verilmiştir.



Şekil – 1 [2]

5.2 2.Yöntem

İkinci yöntem, dijital sinyal işleme (DSP) tabanlı bir fiziksel katman güvenliği şemasıdır [3]. DSP tarafından üretilen bir şifreleme anahtarı tarafından sürülen iki dağıtma elemanı ve bir faz modülatörü (PM) tarafından gerçekleştirilir, sinyal çözme ise ters dağılım değerleri ve güvenlik anahtarları kullanır. DSP tabanlı fiziksel katman güvenliğinin kritik bir yönü, PM'leri veri sinyallerini gizlemeye/kurtarmaya yönlendiren güvenlik anahtarlarının son derece öngörülemez ve gürültüye benzer olması gerektiğidir, bu nedenle ortogonal frekans bölmeli çoğullama (OFDM) sinyalleri kullanıldıkları gibi kullanılır. Şekil – 2'de sistemin şeması yer almaktadır.



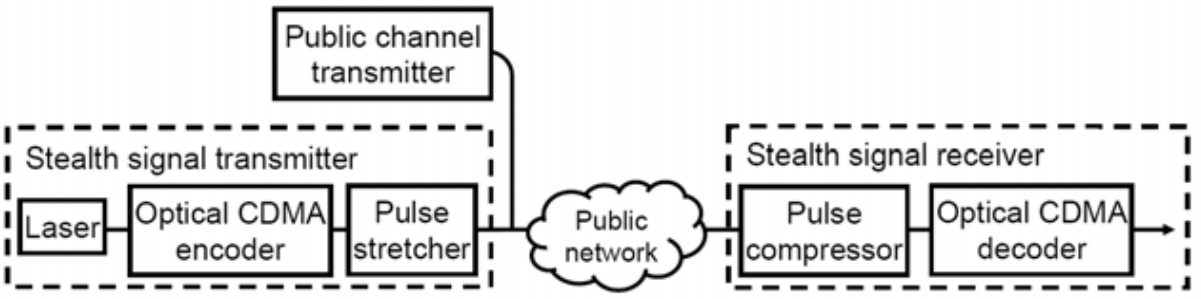
Şekil – 2 [3]

Önerilen sistem, güvenlik anahtarları olarak gerçek zamanlı dijital olarak üretilmiş OFDM sinyallerini kullanır, böylece kaotik sinyalleri anahtar olarak uygulama zorluklarını ortadan kaldırır ve kaotik optik taşıyıcı senkronizasyonunun katı gereksinimlerini ortadan kaldırır. DSP tarafından üretilen OFDM sinyal tabanlı anahtarlar, zaman alanındaki parazit benzeri sinyallerdir ve kurulumdan önce bir güvenlik modülü çiftine önceden programlanan benzersiz ve özel bir parametre setine dayalı olarak üretilir.

5.3 3.Yöntem

Diğer bir yöntem, [5] ve [17]'de görüleceği üzere optik sinyal işleme tabanlı şemadır. Optik sinyal işleme tekniklerini kullanarak, optik iletişim sistemlerinin fiziksel katman güvenliğini geliştiriyoruz. Gerçek zamanlı veri işleme elde etmek için fiber lineer olmama özelliğini kullanarak optik şifrelemeden yararlanılır. Sisteme serpiştirilmiş dalga bandı anahtarlama modülasyonu ve değişken iki kodlu anahtarlama uygulanarak, verilerin güvenliği daha da arttırılır. Yayılmış spektruma dayalı olarak, gizli sinyalin sistem gürültüsü altında iletileceği şekilde optik steganografi de gösterilir. WDM ve optik CDMA sistemlerindeki optik steganografi gösterilmiştir. Ayrıca, yedekleme kanalındaki bant genişliğini boşa harcamadan hizmet kullanılabilirliğini arttıran optik CDMA tabanlı yedekleme kanalları önerilir. Sağlanan çok katmanlı güvenlik, ağın gizliliğini ve kullanılabilirliğini arttırır.

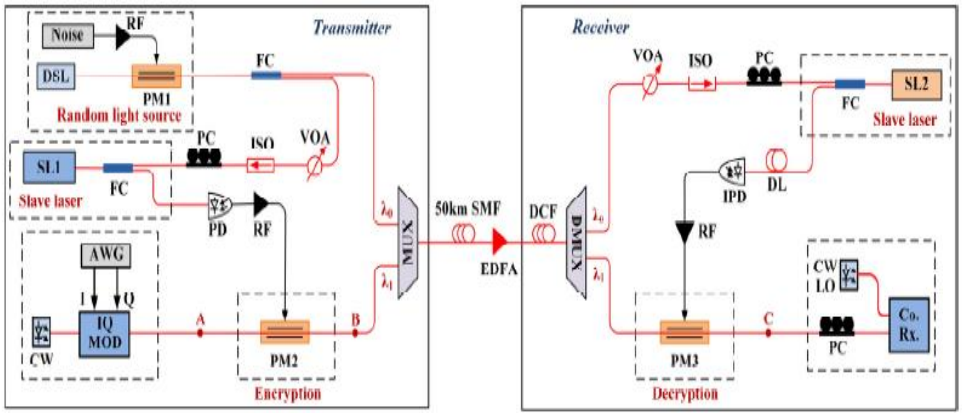
Optik şifreleme, sinyallerin radyo frekansı imzası yaymadan düşük gecikme süresi ve yüksek hızda şifrelenmesini sağlar. Optik steganografi, genel kanalın altında veri iletiminin varlığını gizleyerek veri şifrelemeyi tamamlayabilen ek bir gizlilik katmanı sağlar. Şekil – 3'te önerilen sisteme ait bir şema verilmiştir.



Şekil – 3 [5]

5.4 4.Yöntem

Şimdi ise [20]'deki özel kaotik faz karıştırmasına dayalı bir sistem açıklanacaktır. Deneysel olarak 50 kim'lik tek modlu fiber üzerinden örnek teşkil eden 25 Gbps güvenli QPSK iletimi gösterilmiştir. Burada fiziksel katman şifreleme ve şifre çözme için veri sinyallerini karıştırmak ve çözmek için bir çift ortak enjeksiyon kaynaklı senkronizasyon lazeri tarafından iki özel kaotik sinyal üretilir. Optik XOR mantığı, OCDM teknikleri gibi uygulamaların bazı dezavantajlarının üstesinden gelmek hedeflenmektedir. Önerilen şema ile, iletim verilerinin 0.5 civarından bir doğrudan algılama BER'i ile iyi bir şekilde gizlenebileceğini gösterilmektedir. Şekil – 4'te ilgili şema yer almaktadır.

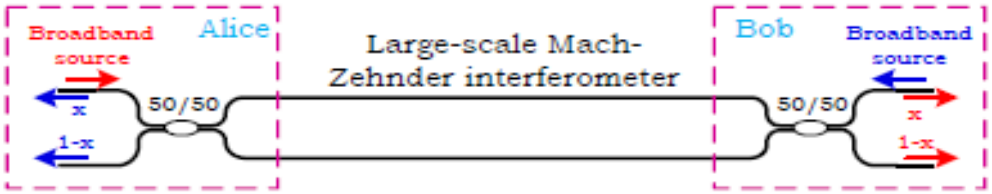


Şekil – 4 [20]

5.5 Gizli Anahtar Üretimi

Fiberdeki faz dalgalanmalarını kullanarak gizli bir anahtar oluşturulmuştur ve elde edilen anahtar, taraflar arasında güvenli iletişimi desteklemek için kolayca kullanılabilir. Yaklaşımın güvenliği, optik fiziksel katmanla ilişkili temel bir asimetriye dayanmaktadır. Kulak misafiri olan bir düşmanın kilit düzeni bozmak için ihtiyaç duyduğu araçların karmaşıklığı, meşru tarafların planı uygulamak için ihtiyaç duyduğu karmaşıklıktan önemli ölçüde daha büyük ve daha maliyetlidir. Günümüzde en çok benimsenen dağıtım yöntemleri, asimetrik veya açık anahtarlı kriptografiye dayanmaktadır.

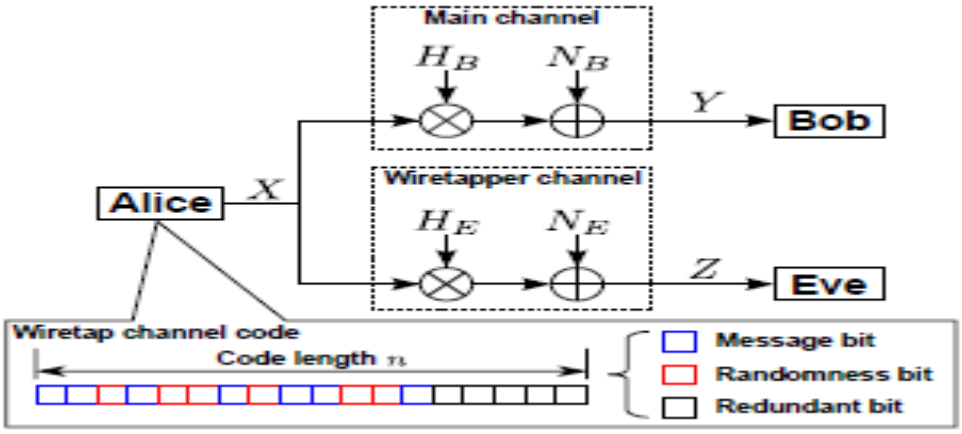
Optik fiziksel katmanın özelliklerini kullanan optik iletişim için gizli anahtar oluşturma şeması sunulmaktadır [8]. Spesifik olarak, yaklaşımımız fiber optik ortamdaki faz dalgalanmalarını izlemeye dayanmaktadır ve saldırganın sistem çalışırken bile sistem hakkındaki tüm olası bilgileri bildiği varsayımı altında çalışmaktadır. Meşru tarafların, kulak misafiri olan bir rakibe ciddi zorluklar empoze etmek için kullanması gereken iş miktarı açısından verimli hale getirir. Şekil – 5'te örnek bir şema yer almaktadır.



Şekil – 5 [8]

5.6 Free Space Optik Fiziksel Katman Güvenliği

Serbest alan optik (FSO) iletişimi, düzensiz bir spektrumda geniş bant genişliği, ultra düşük kanallar arası girişim ve güç verimli iletim gibi özellikler sayesinde kablosuz ağların bağlanabilirliğini geliştirmek için umut verici bir teknolojidir. Lazer ışınının yüksek yönlülüğü, FSO iletişimini doğası gereği RF muadillerinden daha güvenli kılar. Ancak yine de fiziksel katman güvenliği önemli konudur. [19] ve [9]'dan açma-kapama anahtarlama modülasyonuna dayalı sözde rasgele bir ikili dizi ileterek FSO telefon dinleme kanalının özelliklerini analiz edebiliriz. Şekil – 6'da temel yapı görülmektedir.

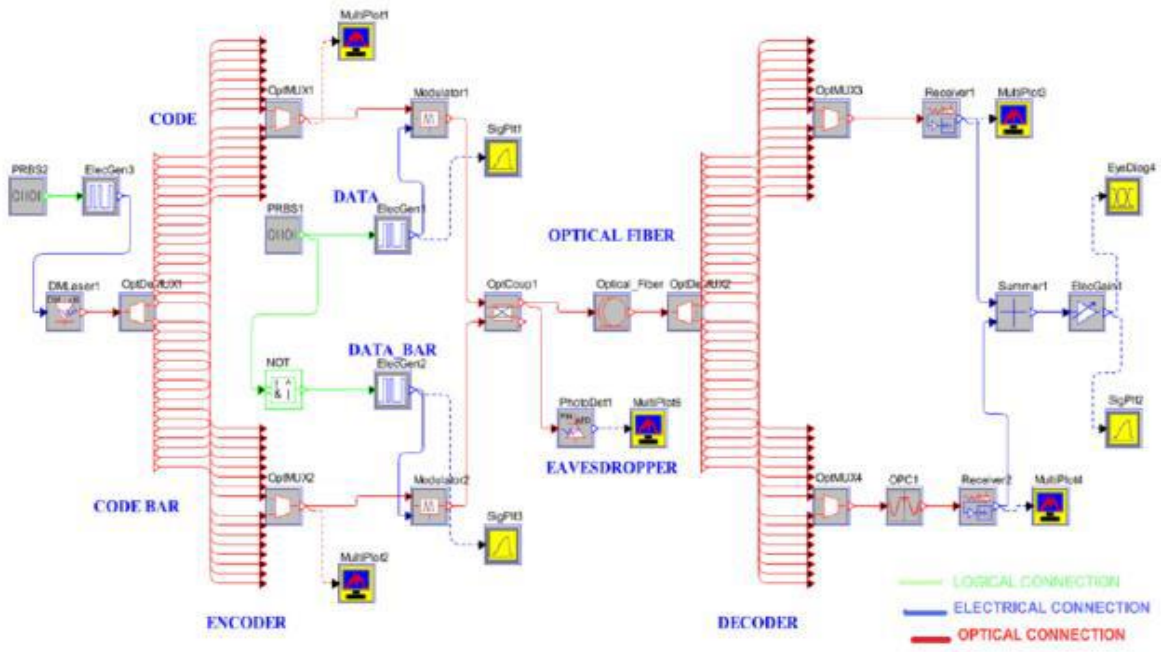


Şekil – 6 [19]

Alternatif bir senaryo olarak, kulak misafirinin daha büyük miktarda güç toplamak için lazer ışınını bloke etmesi olabilir. Böyle bir durumda, yasal alıcı ortalama alınan gücün hissedilir derecede azaldığını farkedecek ve bu nedenle güvenlik nedenleriyle iletişim durdurulabilecektir [9].

5.7 Optik Ağlarda Fiziksel Katman Saldırıları ve Çözüm Yöntemleri

İlk olarak [7]'ye dayanarak OCDMA tabanlı ağlarda kod değiştirme şemaları kullanılmasını inceleyeceğiz. Bu yöntemde, bir kullanıcıya iletilen verilerin kolayca dinleme yapan kişi tarafından okunabileceği gösterilmektedir. Güvenliği arttırmak için bir kod anahtarlamalı şema uygulanmıştır. Şema Şekil – 7'de görülebilir.



Şekil – 7 [7]

Dalga boyu bölmeli çoğullama (WDM) ağlarında temel ilke, [10]'dan farklı dalga boylarının bağımsız kümeleri arasında bölmektir. WDM ağlarında ağ saldırıları şöyle sınıflandırılır.

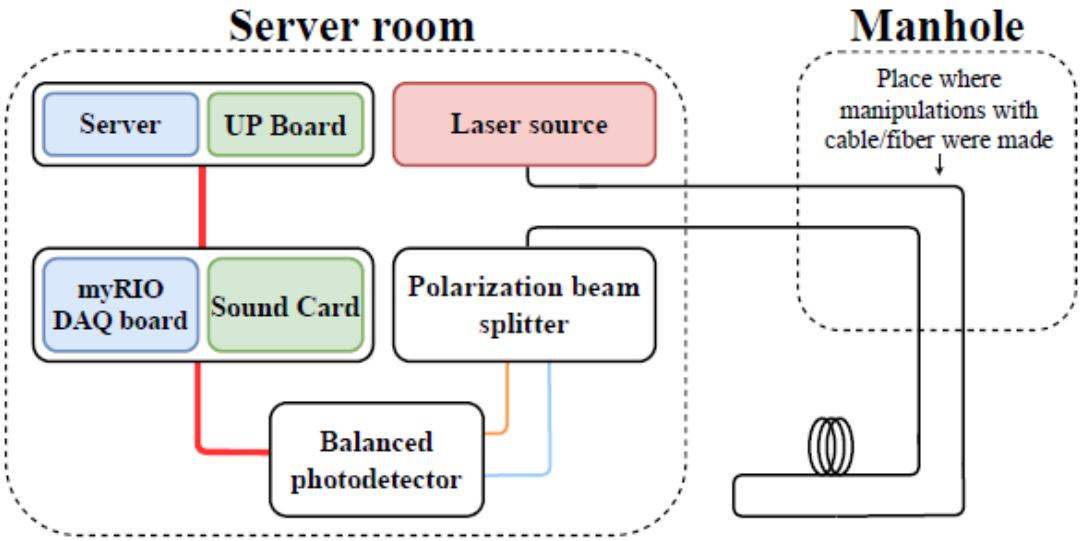
İletişimi engelleyen ve hizmet kalitesini düşüren "Hizmet Kesintisi".

Yetkisiz kullanıcıların verilere erişmesini sağlayarak mahremiyeti tehlikeye atan ve daha sonra gizli dinleme ve trafik analizi için kullanılabilen "Dokunma".

Fiziksel katman saldırıları ise Doğrudan Saldırılar, Ağ iletimini hedefleyen saldırılar, Optik yükselticilere yönelik saldırılar, Optik iletimi hedefleyen saldırılar (Örneğin, fiber kesme), Dolaylı Saldırılar.

Fiziksel katman güvenliğini ihlal eden olayları sınıflandırmak amacıyla [11]'den bir çalışma yapılmıştır. Bu çalışmada, fiziksel katmanın optik kablolarının güvenliğini sağlamak için polarizasyon analizi kullanılmıştır. Bu yöntem, bir polarizasyon ışını ayrıcısı ve dengeleyici bir fotodedektör kullanılarak kolayca tespit edilebilen, polarizasyon durumlarında mekanik titreşimlerin neden olduğu değişikliklerden yararlanılır.

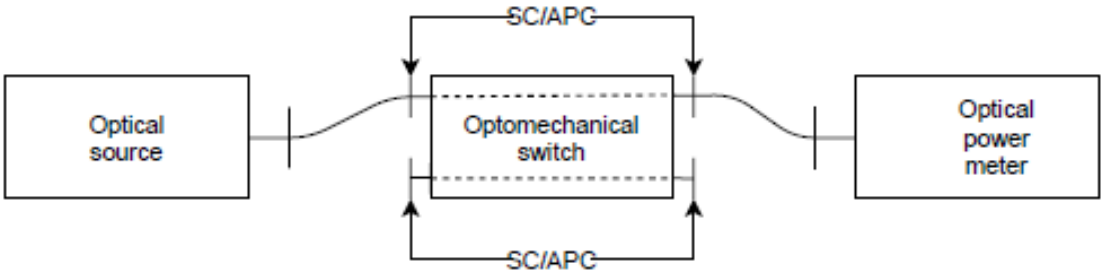
Şekil – 8'de örnek bir şema yer almaktadır.



Şekil – 8 [11]

Optik fiziksel katmanda güvenlik risklerini analiz ettiğimizde, en büyük risk, [14]'ten optik dağıtım ağına bir ayırıcı yerleştirme ve tüm spektrumun bir bölümünü, yani optic fiberdeki tüm kanalları yakalama olasılığıdır. Diğer bir önemli güvenlik riski, dalga boyu bölmeli çoğullamaya sahip ağlardaki çoklayıcılardaki karışmadır.

Optomekanik anahtarların portları arasındaki izolasyon, güvenli veri aktarımını sağlamak için yeterlidir. En büyük potansiyel tehlike, rotaya 1:99 güç ayırıcı yerleştirmektir. Bir saldırıyı gerçekleştirmek için gereken süre nispeten küçüktür ve ekleme kaybı neredeyse tespit edilemez. Şekil – 9'da bir optik anahtarın şeması yer almaktadır.

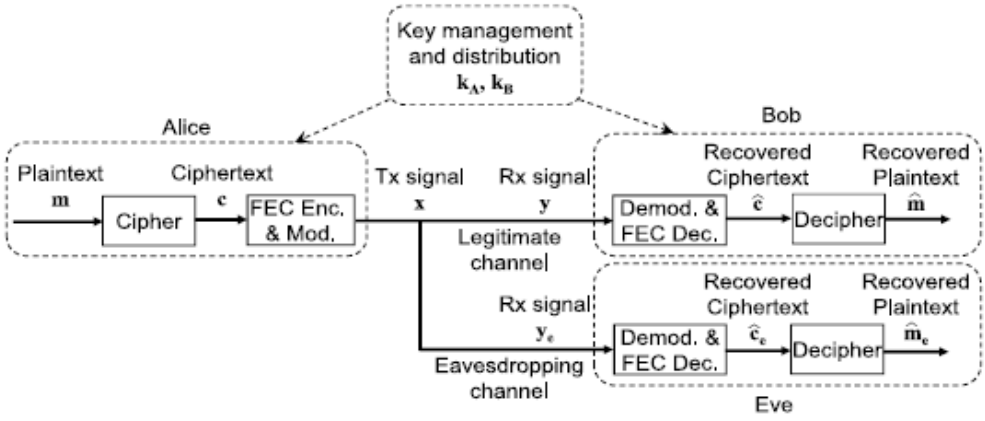


Şekil – 9 [14]

5.8 MIMO-SMD Sistemlerinde Fiziksel Katman Güvenliği

[18]'de anahtar tabanlı ve anahtarsız şifreleme ve fiziksel katman güvenlik teknikleri sınıflandırılmıştır. Bunlar optik çok girişli çok çıkışlı uzay bölmeli çoklama (MIMO-SDM) fiber optik iletişim sistemleri bağlamında tartışılmıştır. Fiber optik MIMO-SDM sistemlerinin fiziksel katman güvenliği ve bükülme kaynaklı MDL'nin farklı anahtarsız şifreleme yaklaşımları aracılığıyla güvenlik amaçları için nasıl kullanılabileceği gösterilmiştir. Alice ve Bob arasındaki gizli bir anahtar dağıtma yöntemleri, güvenilir kurye hizmetlerinden kuantum anahtar dağıtımına (QKD) kadar uzanır.

Şekil – 10'da örnek bir şema gösterilmiştir.



Şekil – 10 [18]

5.9 Optik Kablosuz İletişimde Fiziksel Katman Güvenliği

[4]'ten mevcut RF ağları, sürekli artan veri hızı talebini karşılayamadığından, kullanılmayan geniş bir düzenlenmemiş spektrum kullanan optik kablosuz iletişim (OWC), RF spektrum sınırlamalarının üstesinden gelmek için umut verici bir teknoloji olarak önerilmiştir.

OWC, RF ağlarıyla karşılaştırıldığında LED'lerin sağladığı küçük kapsama alanı nedeniyle daha güvenlidir.

OWC ağlarında güvenlik, özellikle halka açık alanlari toplantı odaları, laboratuvarlar ve kütüphaneler gibi iletilen bilgilere birden fazla kullanıcı tarafından erişilebildiği görünür ışık iletişiminde (VLC) hala bir sorundur.

Fiziksel katman güvenliği, gürültünün rasgeleliğini, kanal durumu bilgisini (CSI) ve farklı kaynakları kullanarak dinleyicilerde elde edilen bilgileri azaltmak için umut verici bir Teknik olarak ortaya çıkmıştır.

OWC sistemlerinde verici olarak genellikle lazerler veya ışık yayan diyotlar kullanılırken, alıcıların alınan ışık yoğunluğunu akım sinyaline dönüştürebilen foto-dedektörlerle donatılması gerekir. FSO ve VLC sistemlerinin PLS mekanizmalarını kullanarak güvenlik altına alınmasına yönelik çalışmalar yapılmıştır.

OWC'nin diğer bir benzersiz özelliği de, iletimin yalnızca görüş hattı (LoS) bileşeni mevcut olduğunda düzgün çalışabilmesidir. Başka bir deyişle, LoS bileşeni yoksa kanal önemli ölçüde bozulur.

5.10 6G ve gelişen Optik Ağlarda Fiziksel Katman Güvenliği

[6] ve [15]'ten diyebiliyoruz ki altıncı nesil (6G) mobil ağ, makro cihazlardan nano cihazlara kadar farklı düğümlerden oluşacak ve etrafımızda tam bir bağlantı dokusu sağlayacak. Bu heterojen düğümler, genellikle çok hassas olan tonlarca bilgiyi yöneten ultra yoğun bir ağ oluşturur.

Bu tür bir ağ tarafından sağlanan hizmetlere güvenmek için güvenlik, tasarım gereği zorunlu bir özelliktir. Bu senaryoda, fiziksel katman güvenliği (PLS), farklı ortamlardaki düşük kaynaklı düğümlere bile güvenlik sağlayarak ilk savunma hattı görevi görebilir.

Bu kapsamda, makine öğrenimi (ML), yapay zeka (AI) ve modern sinyal işlemenin yaklaşan trendlerinden yararlanarak yeni erişim şemaları optimize edilecek olması beklenmektedir.

AI'nin yaygın kullanımı ile birlikte AI teknolojisi uygulanarak, PLS paradigması geleneksel güvenik teknolojilerine kıyasla daha da geliştirilebilir.

Ayrıca gelecekteki dinamik optik ağlarla ilişkili artan karmaşıklığı desteklemek için, kontrol ve yönetimi basitleştirmek için umut verici bir çözüm olarak yazılım tanımlı ağ (SDN) önerilmiştir [16].

SDN paradigması, kontrol ve veri düzlemlerini ayırmaya ve kontrol mantığını yönlendiricilerden ve anahtarlardan, esasen bir ağ işletim sistemi olarak hareket eden, mantıksal olarak merkezi bir denetleyiciye kaydırmaya odaklanır.

Optik ağların dinamik elastic SDN tabanlı ağlara dönüşmesi, güvenli bir ağ ortamı sağlamak için de ele alınması gereken yeni güvenlik açıklarına yol açacaktır.

Henüz bu güvenlik ihlallerine karşı koyabilecek tüm yollar belirlenmemiş olsa da makine öğrenimi ve yapay zeka'nın bu yolda çok önemli başarımlara yol açacağı beklenmektedir.

5.11 Önerilen Özel Fiziksel Katman Güvenliği Şeması

[1]'de yer alan PLS şemasının bu çalışmanın hipotezine en uygun çalışma olduğu görülmektedir. [1]'de Eve'in Alice ve Bob arasındaki kalibrasyona şahit olmasına ragmen güvenli iletimin sağlanmasına yönelik bir çalışma anlatılmıştır.

Fiber optik bir ağda çok modlu fiberlerin (MMF) kullanılması, uzun mesafeli iletimde bile veri hızlarını önemli ölçüde arttırmak için önemli bir yaklaşımdır. MMF'te elyafın bir tarafındaki MMF'e tutarlı ışık gönderildiğinde, MMF'in diğer tarafında benek deseni adı verilen granül bir yapı olarak görünecektir. Bu engel esasında dalga cephesi şekillendirme (WS) kullanılarak aşılabilir.

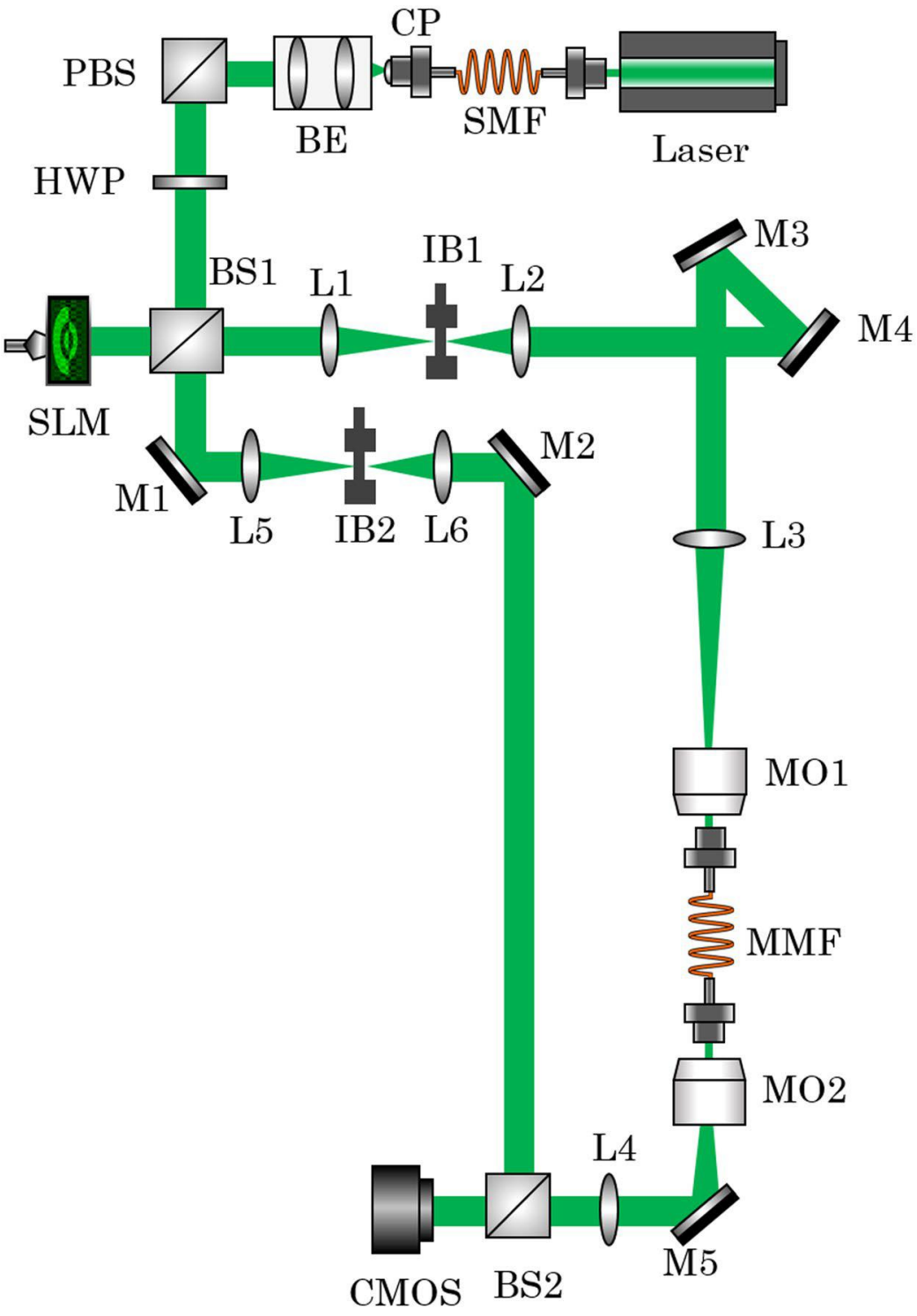
Çok modlu fiberlerde ışığın saçılması genellikle girişim olarak görülür, ancak saçılma özellikleri rasgele olduğundan bilgi güvenliği seviyesini arttırmak için kapıyı açabilirler.

Bu nedenle, Alice ve Bob arasındaki iletim kanalını WS kullanarak kontrol ederek, fiberin merkezinde bir yerde sinyali alan Eve, yalnızca karıştırılmış bir benek modeli alacaktır. Ek olarak, bu fikir düşük bir foton sayısıyla birlikte araştırılmıştır, böylece Eve bilginin yalnızca bir ksımını alır.

Önerilen bu çalışmada, PLS, yapay gürültü ile ters ön kodlama kullanılarak uygulanır. Bu Eve (illegal kulak misafiri) kanallar hakkında tam bilgiye sahip olsa bile güvenli iletişim sağlar. Bunun anahtarı, MMF'ler içindeki kanal davranışı için karakteristik olan moda bağlı kayıpların kullanılmasıdır. Bob, gönderilen modları doğrudan gözlemlerken, Eve'in Matrix İnversion kullanması gerekir. Bu Alice'e yapay gürültü getirme ve böylece Eve'in algıladığı gürültüyü arttırma gücü verir.

Bu, dinamik kanal değişiklikleri kullanıldığında güvenli olarak kabul edilebilecek 4 mod kanalı oluşturacak kadar yüksek olan Bob için bir SNR avantajı ile sonuçlanır.

Güvenli olarak sınıflandırılan 2 kanal kullanıldığı sürece, tüm mod etki alanından 3 kanal üzerinden mesajlar güvenli bir şekilde gönderilebilir. Bu sonuçlar, veri merkezleri ve siber fiziksel sistemler üzerinde potansiyel etkisi olan optik iletim kanallarındaki güvenliği arttırmak için çok önemli bir ilerlemeyi temsil etmektedir. Şekil – 11'de önerilen sistemin kurulum şeması yer almaktadır.


CP
PBS
BE
SMF
Laser
HWP
M3
IB1
BS1
L1
L2
M4
SLM
M2
M1
L5
IB2
L6
L3
MO1
MMF
MO2
L4
M5
CMOS
BS2

Şekil – 11 [1]

6
ARAŞTIRMA YÖNTEMİ

Bu araştırma projesi kapsamında nicel araştırma yöntemi uygulanmıştır. Araştırmacı, olay ve olgulara dışarıdan bakmış ve nesnel bir tavır sergilemiştir. Belirtilen kaynaklardaki deneysel ve hesaplamalı sonuçlara sadık kalınarak nesnel bir şekilde okuyucu ile bunlar paylaşılmıştır.

Toplanan kaynak dökümanlar sayısal verileri dikkate alınarak analiz edilmiştir. Veriler sayısal göstergelere indirgenmiştir.

Konu ile ilgili yapılan teorik ve deneysel çalışmalar incelenmiş ve bunlar konu kapsamında proje içinde okuyucu ile bilimsel bir anlayış çerçevesinde paylaşılmıştır.

Bu kapsamda kaynaklarda da belirtilen kuramlar esas alınarak yöntemler analiz edilmiş ve karşılaştırmalar yapılmıştır.

7
VERİ TOPLAMA YÖNTEMLERİ

Bu proje kapsamında veri toplama yöntemi olarak doküman inceleme yöntemi kullanılmıştır. Doküman inceleme, araştırması hedeflenen olgu ve olgular hakkında bilgi içeren yazılı materyallerin analizini kapsar.

Bu kapsamda öncelikle internet üzerinden IEEE vb. sitelerden konu ile ilgili makalelere ulaşılmıştır. Daha sonra bu makalelerin orjinalliği, güvenilirliği vb. kontrol edilmiştir. Makalelerin anlaşılabilir olduğu kontrol edildikten sonra veriler analiz edilmiştir. Makalelerden elde edilen veriler konu kapsamında kategorize edilmiştir. Sonrasında araştırma projesi kapsamında okuyucuya sunulmuştur. Makale dışında 1 adet de kitap kaynak olarak yer almaktadır.

8
KAYNAKÇA

[1] S. Rothe, N. Koukourakis, H. Radner, A. Lonnstroom, E. Jorswieck, and J. W. Czarske, “Physical Layer Security in Multimode Fiber Optical Networks,” SCIENTIFIC REPORTS, Vol. 10, February 2020.

[2] V. Marudhai, S. Prince, and S. Kumari, “Design and Simulation of Physical Layer Security for Next Generation Intelligent Optical Networks,” Wireless Personel Communications, Vol. 1, June 2021.

[3] J. He, R. Giddings, W. Jin, and J. Tang, “DSP-Based Physical Layer Security For Coherent Optical Communication Systems,” IEEE Photonics Journal, Vol. 14, October 2022.

[4] M. Obeed, A. M. Salhab, M. S. Alouini, and S. A. Zummo, “Survey on Physical Layer Security in Optical Wireless Communication Systems,” 2018 Seventh International Conference on Communications and Networking (ComNet),2018.

[5] P.R. Prucnal, M. P. Fok, Y. Deng, and Z. Wang, “Physical Layer Security in Fiber Optic Networks Using Optical Signal Processing,” 2009 Asia Communications and Photonics Conference and Exhibition (ACP), Vol. 7632, November 2009.

[6] M. Mitev, A. Chorti, S. Member, H. V. Poor, L. Fellow, and G. Fettweis, “What Physical Layer Security Can Do For 6G Security,” IEEE Open Journal Of Vehicular Technology, Vol. 4, pp. 375-388, February 2023.

[7] M. Koca, İ.Avcı, Z.Y. Çavdar, and M.A. Aydın, “A Survey Of Optical Networks Vulnerabilities and Solutions,” 8th International Advanced Technologies Symposium, May 2017.

[8] K. Kravtsov, Z. Wang, W. Trappe, and P.R. Prucnal, “Physical Layer Secret Key Generation For Fiber Optical Networks,” Optics Express, Vol. 21, pp. 23756-23771,2013.

[9] F.J. Lopez-Martinez, G. Gomez, and J.M. Garrido-Ballsells, “Physical Layer Security in Free Space Optical Communications,” IEEE Photonics Journal, Vol. 7, April 2015.

[10] M. Furdek, and N.S. Kapov, “Physical Layer Attacks in Optical WDM Networks and Attack Aware Network Planning,” 2011 Proceedings of the 34th International Convention, 2011.

[11] M. Ruzicka, L. Jabloncik, P. Dejdar, A. Tomasov, V. Spurny, and P. Munster, "Classification of Events Violating the Safety of Physical Layers in Fiber Optic Network Infrastructures," Sensors, 2022.

[12] M. Mitev, T. M. Pham, A. Chorti, and A.N. Barreto, "Physical Layer Security – from Theory to Practice," TechRxiv Powered by IEEE, 2022

[13] D. Sharma, and S.K. Singh, "Optical Network System Existence in Optical Network Systems," International Research Journal of Engineering and Technology, Vol. 7,September 2020.

[14] V. Spurny, P. Munster, A. Tomasov, T. Horvath, and E. Skaljo, "Physical Layer Components Security Risks in Optical Fiber Infrastructures," Sensors, 2022.

[15] L. Mucchi, S. Jayousi, S. Caputo, E. Panayirci, S. Shahabuddin, J. Bechtold, A. Stoica, and G. Abreu, "Physical layer Security in 6G Networks," IEEE Open Journal of the Communications Society, Vol. 2, pp. 1901-1914, August 2021.

[16] N. S. Kapov, M. Furdek, S. Zsigmond, and L. Wosinska, "Physical Layer Security in Evolving Optical Networks," IEEE Communications Magazine, Vol. 54, pp. 110-117, August 2016.

[17] M. P. Fok, Z. Wang, Y. Deng, and P. R. Prucnal, "Optical Layer Security in Fiber Optic Networks," IEEE Transactions on Information Forensics and Security, Vol. 6, pp. 725-736, April 2011.

[18] K. Guan, J. Cho, P. J. Winzer, "Physical Layer Security in Fiber Optic MIMO-SDM Systems : An Overwiev," Optics Communications, Vol. 408, pp. 31-41, February 2018.

[19] H. Endo, M. Fujiwara, T. Ito, M. Toyoshima, and N. Laurenti, "Free Space Optical Channel Estimation for Physical Layer Security," Optics Express, Vol. 24, pp. 8940-8955,2016.

[20] A. Zhao, N. Jiang, Y. Zhang, and K. Qiu, "Physical Layer Secure Optical Communication Based On Private Chaotic Phase Scrambling," 26th Optoelectronics and Communications Conference, 2021.

[21] S. Özsoy, FİBER OPTİK, Birsen Yayınevi, İstanbul, 2009.

9
KAYNAKLARIN GÜVENİLİRLİĞİ

[1] Bu kaynak 2020 yılında Scientific Reports adlı uluslararası bir dergide yayınlanmıştır. Ayrıca makaledeki çalışma Alman Araştırma Kuruluşu (DFG) tarafından desteklenmiştir. Yazarlar, Dresden Teknik Üniversitesi Elektrik ve Bilgisayar Mühendisliği bölümü öğretim görevlileridir. Bu makale 48 referans kaynak göstermiştir.

[2] Bu kaynak 2021 yılında Wireless Personel Communications dergisinde yayınlanmıştır. Yazarlar, Hindistan'da SRM IST Elektronik ve Haberleşme Mühendisliği bölümünde öğretim görevlileridir. Bu makale 28 referans kaynak göstermiştir.

[3] Bu makale IEEE Photonics Journal'de yayınlanmıştır. Yazarlar, Bangor Üniversitesi Elektronik Mühendisliği ve Bilgisayar Bilimleri bölümünde öğretim görevlileridir. Bu makale 28 referans kaynak göstermiştir.

[4] Bu konferans yazısı, 7. Uluslararası Haberleşme ve Networking Konferansı (Suudi Arabistan) dolayısıyla yazılmıştır. Yazarlar, Kral Fahd Bilim ve Teknoloji Üniversitesi öğretim görevlileridir. Bu makale, 58 referans kaynak göstermiştir.

[5] Bu makale, 2009 Asya Haberleşme ve Fotonik dergisinde yayınlanmıştır. Yazarlar, ABD Princeton Üniversitesi Elektrik Mühendisliği bölümü öğretim görevlileridir. Bu makale, 19 referans kaynak göstermiştir.

[6] Bu kaynak, IEEE Taşıt Teknolojisi Dergisi'nde yayınlanmıştır. Yazarlar, Almanya Barkhausen Üniversitesi, ABD Princeton Üniversitesi ve Fransa CY Cergi Paris Üniversitesi'nde öğretim görevlileridir. Bu makale, 33 referans kaynak göstermiştir.

[7] Bu kaynak, Elazığ 8. Uluslararası Gelişmiş Teknolojiler Sempozyumunda yayınlanmıştır. Yazarlar, Hakkari Üniversitesi, İstanbul Üniversitesi ve İstanbul Şehir Üniversitesi öğretim görevlileri ve bir THY IT Departmanı çalışanından oluşmaktadır. Bu kaynak, 21 referans kaynak göstermiştir.

[8] Bu kaynak, Optic Express dergisinde yayınlanmıştır. Yazarlar, Rusya Bilim Akademisi, ABD Rutgers Üniversitesi ve ABD Princeton Üniversitesi öğretim görevlileridir. Bu kaynak, 44 referans kaynak göstermiştir.

[9] Bu kaynak, IEEE Fotonik Dergisinde yayınlanmıştır. Yazarlar, Granada Üniversitesi ve Malaga Üniversitesi öğretim görevlileridir. Bu kaynak, 36 referans kaynak göstermiştir.

[10] Bu kaynak, 2011 Uluslararası Kongre Bildirgesinde yayınlanmıştır. Yazar, Hırvatistan Zagreb Üniversitesi'nde öğretim görevlisidir. Bu kaynak, 23 referans kaynak göstermiştir.

[11] Bu kaynak 2022 yılında Sensörler adlı dergide yayınlanmıştır. Yazarlar, Çin Halk Cumhuriyeti Brno Teknoloji Üniversitesi Elektronik ve Haberleşme Mühendisliği bölümü öğretim görevlileridir. Bu kaynak, 39 referans kaynak göstermiştir.

[12] Bu kaynak IEEE TechRixv açık kaynak havuzunda yayınlanmıştır. Yazarlar, Bulgaristan Varna Üniversitesi , İrlanda Maynooth Üniversitesi ve Brezilya Katolik Üniversitesi öğretim görevlilerinden oluşmaktadır. Kaynak, 30 referans kaynak göstermiştir.

[13] Bu kaynak, Uluslararası Mühendislik ve Teknoloji Araştırma Dergisinde 2020 yılında yayınlanmıştır. Yazarlar, Monad Üniversitesi Yüksek Lisans Öğrencisi ve Bihar Üniversitesi öğretim görevlisinden oluşmaktadır. Bu kaynak, 11 referans kaynak göstermiştir.

[14] Bu kaynak, Optik Fiber Altyapılarında Fiziksel Güvenlik Riskleri dergisinde yayınlanmıştır. Yazarlar, Bosna Hersek Sarajevo Üniversitesi ve Çin Halk Cumhuriyeti Brno Teknoloji Üniversitesi öğretim görevlileridir. Bu kaynak, 16 referans kaynak göstermiştir.

[15] Bu kaynak, 2021 yılında IEEE Haberleşme Dergisinde yayınlanmıştır. Yazarlar, IEEE Kıdemli üye ve üyelerinden ve eşlerinden oluşmaktadır. Bu kaynak, 86 referans kaynak göstermiştir.

[16] Bu kaynak, 2016 yılında IEEE Haberleşme Dergisinde yayınlanmıştır. Yazarlar, San Javier Hava Kuvvetleri Savunma Üniversitesi'nde ve Kraliyet Teknoloji Enstitüsünde öğretim görevlilerinden ve bir Nokia çalışanından oluşmaktadır. Bu kaynak, 15 referans kaynak göstermiştir.

[17] Bu kaynak, IEEE Adli Tıp ve Güvenlik dergisinde yayınlanmıştır. Yazarlar, IEEE üyelerinden oluşmaktadır. Bu kaynak, 60 referans kaynak göstermiştir.

[18] Bu kaynak, Optik Haberleşme adlı bir dergide yayınlanmıştır. Yazarlar, ABD Nokia Bell Laboratuvarı çalışanlarıdır. Bu kaynak, 59 referans kaynak göstermiştir.

[19] Bu kaynak, Optic Express adlı bir dergide yayınlanmıştır. Yazarlar, Japonya Uluslararası Bilgi ve Haberleşme Üniversitesi , Tokai Üniversitesi, Elektronik Haberleşme Üniversitesi öğretim görevlilerinden oluşmaktadır. Bu kaynak, 38 referans kaynak göstermiştir.

[20] Bu kaynak, 2021 Optoelektronik ve Haberleşme Konferansında yayınlanmıştır. Yazarlar, Çin Elektronik Bilimi ve Teknoloji Üniversitesi öğretim görevlileridir. Bu kaynak, 8 referans kaynak göstermiştir.

[21] Bu kaynak, Prof. Dr. Sedat Özsoy tarafından yazılmıştır. Prof. Dr. Sedat Özsoy, Erciyes Üniversitesi Fizik Bölümü öğretim görevlisidir. Kitabın ismi FİBER OPTİK'tir. Kitap, Birsen Yayınevi tarafından 2009 yılında yayınlanmıştır.