

Derin Sır – Kuantum Seviyesinde Güvenli Denizaltı İletişimi

Kuantum anahtar dağıtım teknolojisi, denizaltıların hem derinlikte hem de hızda güvenli bir şekilde iletişim kurmasını sağlayabilir. Berenice Baker, fizik yasalarının kendisi tarafından korunan bir gizlilik düzeyinde sualtı iletişiminin ne kadar hızlı sağlanabileceğini araştırıyor.

[Berenice Baker](#) tarafından



Denizaltı İletişim Zorlukları

Denizaltı iletişimi, gemilerin bilgi alışverişinde bulunabilecekleri derinlik ve bunu su aracılığıyla yapabilecekleri hız ile sınırlıdır.

Ancak son zamanlarda, araştırmacılar Kuantum Anahtar Dağılımı (QKD) adı verilen bir teknik kullanarak bu ikilemi çözmede etkileyici adımlar attılar.

QKD, hızdan ödün vermeden veya denizaltıyı yüzeye daha yakın yükselmeye zorlamadan kuantum mekaniği ilkeleri aracılığıyla güvenli iletişimi garanti etmeyi vaat ediyor.

"Denizaltı iletişimi, gemilerin bilgi alışverişinde bulunabileceği derinlikle sınırlıdır."

Bir denizaltının tüm taktik avantajını koruyabilmesi için, 60 ila 100 metre derinliğinde olan ve altındaki yüzey sonarlarının onları tespit edemediği karışık katmana batmış durumda kalması gerekir. Denizaltı iletişimi şu anda ELF veya VLF radyo dalgaları kullanılarak batık halde gerçekleştirilmektedir, çünkü bu derinliklerde suya yalnızca çok düşük veya aşırı düşük frekanslar nüfuz edebilir.

Bununla birlikte, ELF ve VLF'nin kullanılması bir takım dezavantajlar sunar. İletim alanları çok büyük olmalıdır, yani denizaltı hantal anten kabloları çekmeli ve ayrıca optimum alımı elde etmek için genellikle belirli bir yöne hizalanmalı ve hızı azaltmalıdır.

VLF ve ELF frekansları yalnızca çok düşük bir bant genişliği sunar: VLF saniyede birkaç yüz biti desteklerken, ELF her dakika yalnızca birkaç biti destekler. Bu, video gibi karmaşık verilerin iletilmesini önler.

Potansiyel bir çözüm, bir denizaltı ve havadaki bir platform arasında bir optik kanalın sürdürülmesinin mümkün olduğunu göstermek için deneylerin yapıldığı 1980'lerden beri var olan bir kavram olan lazer kullanarak optik iletişim gerçekleştirmektir.

Savunma teknolojisi uzmanı ITT Exelis'teki Quantum Technologies grubu, bir denizaltı ile bir uydu veya bir hava platformu arasında kuantum bilgisi kullanılarak güvence altına alınan lazer optik iletişimin fizibilitesini araştırarak bunu bir adım daha ileri götürmekle ilgileniyor.

ITT Exelis'in ABD Hükümeti için yürüttüğü çalışma, kuantum algoritmalarının geliştirilmesi, kuantum sensörleri ve kuantum iletişim sistemleri için yeni çözümler de dahil olmak üzere çok çeşitli kuantum bilgi konularında araştırmaları içeriyor.

Mükemmel güvenli anahtarlar

ITT Exelis'in Bilgi Sistemleri bölümündeki Quantum Technologies grubunun yöneticisi Dr. Marco Lanzagorta, QKD'nin bir çift mükemmel güvenli anahtar oluşturmak için kuantum bilgisini kullanan bir protokol olduğunu açıklıyor.

" Kuantum bilgisi klasik bilgiden farklıdır, çünkü klasik bilgide birim bittir ve sıfır veya bir değerine sahip olabilir" dedi. "Kuantum bilgisinin birimi, bir fotonun kuantum hali olan kübittir. Sıfır, bir veya sıfır ve birin herhangi bir süperpozisyonu üzerinde olabilir. Klasik olandan daha çok bir bilgi kavramı."



Ohio Sınıfı denizaltılar, Amerika Birleşik Devletleri Donanması'na kıtalararası füzelerin neredeyse algılanamayan denizaltı fırlatma platformları olarak hizmet ediyor.

Kuantum bilgisi, iletişimi güvence altına almak için iki önemli özelliğe sahiptir. Kopyalanamaz, yani sahte olamaz ve bir kuantum durumu bir gözlemci tarafından her ölçüldüğünde çöker, bu da özelliklerinin tespit edilmesinin çok zor olduğu anlamına gelir.

"QKD, hızdan ödün vermeden kuantum mekaniği ilkeleri aracılığıyla güvenli iletişimi garanti etmeyi vaat ediyor."

QKD'de bir araya getirilen bu özellikler, mükemmel güvenli anahtarlar oluşturmak için kullanılabilir, çünkü anahtarların gizliliği fizik yasaları tarafından garanti edilir. Lanzagorta, kamusal alan sistemi RSA, Diffie-Hellman ve ElGamal şifreleme yöntemleri gibi geleneksel şifreleme sistemlerinde güvenliğin çok zor bir matematik probleminin çözümüne dayandığını açıklıyor. Ancak, bu matematiksel problemin, örneğin RSA durumunda asal çarpanlara ayırmanın, gelişmiş bir algoritma tarafından kırılmayacağına dair resmi bir kanıt yoktur.

Ayrıca varsayımsal kuantum bilgisayarların bu tür şifreleri katlanarak daha hızlı kırabileceği tahmin ediliyor. Dolayısıyla QKD, rakipsiz bir şekilde güvenli bir çözüm sunacaktır.

optik iletişim

QKD teknolojisi zaten mevcuttur ve ticari olarak mevcuttur, ancak şu anda havada veya suda serbestçe dolaşan fotonlar yerine bir optik fiber aracılığıyla yürütülmektedir.

"Boş alanda hareket eden fotonlar kullanılarak QKD üzerinde bazı deneyler yapıldı" dedi. "Son zamanlarda Kanarya Adaları'nda 144km mesafede ilk temel QKD'yi yaptıkları bir deney yapıldı ve bu boş alan kuantum iletişimine sahip olmanın mümkün olduğunu gösterdi.

"QKD'de bir araya getirilen bu özellikler, anahtarların gizliliği garanti edildiğinden, mükemmel şekilde güvenli anahtarlar oluşturmak için kullanılabilir."

"Yerdeki bir siteyi bir uydu platformuna bağlamak için başka çalışmalar da yapıldı, ancak biz bir yer platformunda değil, suya batmış bir platformda çalışıyoruz."

Su ve serbest hava yoluyla fotonları iletmenin zorluklarına ek olarak, araştırmacıların uydu veya hava platformundaki verici ile alıcı arasında bir lazer bağlantısı kurması gerekiyor.

Bu, şu anda uzman bir izleme sistemi geliştiren bir QinetiQ Kuzey Amerika ekibi tarafından ele alınmaktadır.

Denizaltı ve uydu arasındaki optik bağlantı kurulduğunda, ITT Exelis araştırmacılarının işi devralır ve QKD protokolünün iletişimi güvence altına almak için nasıl etkinleştirileceğini

araştırır. Bu, Geiger modu olarak bilinen, belirli bir polarizasyona ulaşan fotonları saydığı anlamına gelen bir fotosensör kullanılarak yapılır.

" Kuantum bilgisinin iletilmesi için, fotonları polarize edecek bir şeye ihtiyacınız var, böylece kuantum durumu belirli bir temelde olacak ve bunu verici ve alıcıda algılayan bir filtreye sahip olacaksınız" dedi.

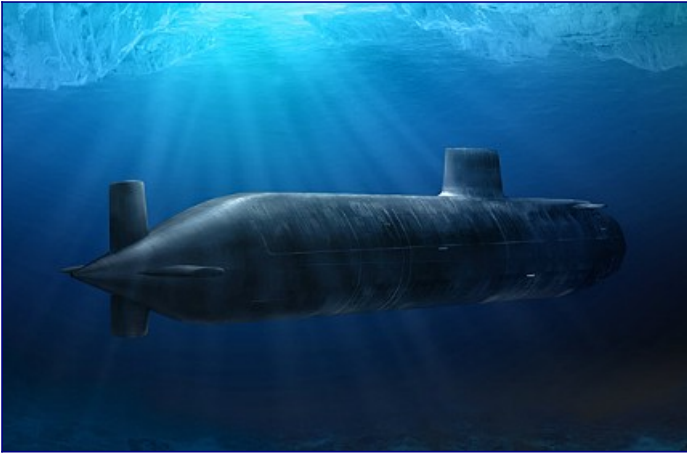
" Çok seyreltilmiş bir lazere benzeyen özel foton lazerlere ihtiyacınız olduğu için normal lazerleri kullanamazsınız. Bunlar her seferinde bir foton gönderir ve her fotonun iyi belirlenmiş bir kuantum durumu vardır."

Fizibilite çalışmaları

Programın bir sonraki aşaması, ABD Deniz Araştırma Laboratuvarı'nın, bir fotonun kuantum durumunun su içinde ilerlerken ne kadar iyi korunduğunu belirlemek ve ITT Exelis'in teorik fizibilite çalışmasının doğruluğunu doğrulamak için bir dizi deney gerçekleştirmesini görecektir.

Deneyler teorik modeli desteklerse ve araştırma bir sonraki aşamaya geçerse, beş yıl içinde deneysel bir prototip yer alabilir. Bununla birlikte, böylesine radikal bir yeni yaklaşımda bir dizi faktör rol oynamaktadır.

Lanzagorta, " Bu yalnızca bilimsel bir teknolojik soru değil, aynı zamanda finansman düzeyleri ve politikayla da ilgili" dedi.



Kraliyet Donanması'nın Astute Sınıfı denizaltısı, nükleer enerjiyle çalışan bir saldırı denizaltısıdır.

Bununla birlikte, yetkiler bunu görürse, faydalar önemli olabilir. Önerilen sistem, video gibi karmaşık verilerle kolayca başa çıkabilen mevcut VLF sistemlerinin kapasitesinden yaklaşık 600 kat daha fazla bant genişliği olan saniyede 170 kb'ye varan hızlarda, mevcut en yüksek güvenlik seviyesi olan mükemmel güvenli iletimi potansiyel olarak sağlayabilir.

Ek olarak, prensipte yavaşlaması, 100 m'den daha az derinlikte kalması veya veri alışverişi için yönünü değiştirmesi gerekmeyeceğinden, denizaltının kendisi için operasyonel verimlilik veya gizlilik kaybı olmayacaktır.

Bu faktörler, QinetiQ tarafından ele alınan çözümün verici lazer ve alıcı sistem kısmı tarafından ele alınacaktır.

Bununla birlikte, tüm başarı, suda seyahat etmenin fotonu nasıl etkilediğine bağlıdır. Lanzagorta, "En büyük zorluk, tek foton darbelerini kuantum halinin sudan geçse bile korunacağı şekilde göndermenin en iyi yolunun ne olduğunu görmektir" dedi. "Daha geniş bir operasyon yelpazesine sahip olabilmemiz için fotonun kuantum durumunu koruyan hata düzeltme kodlaması gibi bir tür kodlama yapmanın bir yolunu bulmamız gerekiyor."