Denizcilik Sektöründe Uydu Tabanlı İletişimin Bilgi Güvenliği ve Şifrelenmesi

Özkan Kılıç, Ali Solak, Hamza Gerçekcioğlu

***Özet* - İletişim teknolojileri ve kesintisiz iletişim denince son dönemde akla ilk olarak uydu teknolojileri gelmektedir. Uydu teknolojilerinin en yaygın olarak kullanıldığı alanlardan birisi de denizcilik sektörüdür. Ülkemizde denizcilik sektörünün kamu yararı açısından stratejik önem taşıması, bu sektörün gelişmesine yönelik bilgi ve teknoloji transferi ile birlikte, üniversite, kamu ve özel sektörün yeteneklerinin birleştirilerek uygulanabilir projeler geliştirilmesine dayanak oluşturmuş, uydu sistemlerinin güncel uygulamalarda kullanılmasına yol açmıştır. Ülkemizde son yıllarda uydu teknolojilerinin kullanıldığı bir diğer alan da Arama Kurtarma harekatlarıdır. Ülkemizdeki Arama Kurtarma kabiliyetine ek olarak mevcut sistemler COSPAS/SARSAT uydu yardımlı arama kurtarma sistemleri ile de desteklenmiştir. Bu çalışmada, denizcilik sektöründe AIS(Otomatik Tanımlama Sistemi), LRIT (Uzun Mesafe Tanımlama ve İzleme), VTMIS(Deniz Araçları Trafiğini İzleme, Yönetme ve Tanımla Sistemleri), INMARSAT teknolojilerinde uydu sistemlerinin nasıl kullanıldığı ve bu sistemlerin genel teknik özellikleri, bilgi güvenliği uygulamaları ve avantajları, mevcut bilgi transferinin hata düzeltme ve şifreleme yöntemi ile gerçekleştirilmesi gerektiğinden ve verimliliğinden bahsedilecektir.**

Anahtar Kelimeler: Hata düzeltme, Şifreleme, Uydu yardımlı iletişim teknolojileri

I. GİRİŞ

Uydu teknolojisi, iletişim teknolojileri arasında alışılmışın dışında, yalnızca askeri amaçlı değil sivil hayatta da hızla kullanım alanları içerisinde yer almaktadır. Güncel her türlü ihtiyacın içinde yer alan bu teknoloji araç ve filo takip sistemleri, deniz ve hava araçlarının izlenmesi, taşımacılık ve haberleşme başta olmak üzere eğitimden sağlığa ve yayıncılığa kadar pek çok alanda vazgeçilmez olmuştur.

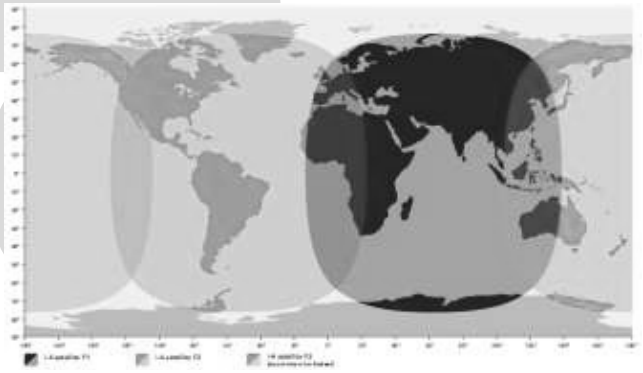
Denize kıyısı olan bütün ülkeler için bu sektörde kullanılan uydu teknolojisi temelli iletişim kanalları büyük önem taşımaktadır. Gerek kendi karasularında seyreden gemiler gerekse diğer ülkelerin karasularında seyreden kendi ülkesine ait veya ait olmayan gemilerin izlenip tanımlanması ve gerekmesi halinde birçok farklı iletişim olanakları ile temas kurulması ihtiyacı, bu temasın denizcilik sektöründeki iletişim olanaklarının daha kaliteli, kesintisiz , dolayısı ile uydu tabanlı olması zorunluluğunu doğurmuştur [1].

Özkan Kılıç, Bilgisayar Mühendisliği Bölümü, Atılım Üniversitesi,
Ali Solak, Denizcilik Müsteşarlığı
Hamza Gerçekcioğlu, Denizcilik Müsteşarlığı

Denizcilik sektöründe kullanılan teknolojilerin çoğunun temeli uydu tabanlı iletişime dayanmakta ve iletişim güvenliğine ihtiyaç duymaktadır. Bu teknolojilerin başlıcaları olan INMARSAT, AIS, LRIT, VTMIS, COSPAS/SARSAT, sistemlerinin teknik özellikleri aşağıda verilmiştir. Bu teknik bilgilerden sonra, bahsedilen sistemlerde hata düzeltme ve bilgi güvenliği konusu tartışılacaktır.

II. UYDU TABANLI SİSTEMLER ve ÖZELLİKLERİ

Uydu teknolojilerinin Denizcilik Sektörü'nde kullanıldığı alanların başında INMARSAT sistemleri gelmektedir. INMARSAT sistemleri, Geostationary konumda dünyadan 35,786 km yukarıda yer alan 10 adedi operasyonel olarak faaliyet gösteren ve kontrol merkezi Londra da olmak üzere, dünyanın herhangi bir yerinde hava, kara, deniz üzerinde bulunan kullanıcı ile mobil iletişim ve yüksek hızda data iletim hizmeti veren uydu destekli haberleşme sistemidir [2]. **Şekil 1**'de INMARSAT uydularının kapsama alanları görülmektedir.

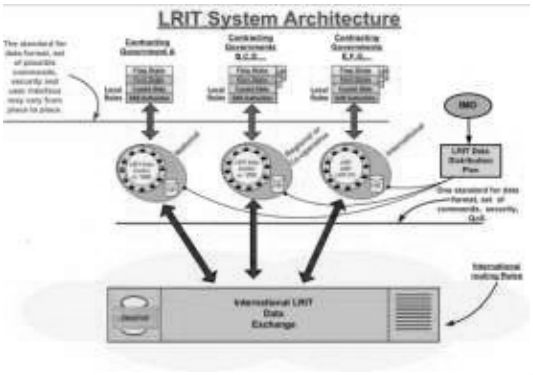


Şekil 1 INMARSAT Uyduları Kapsama Alanı

Diğer bir sistem olan LRIT[1] (Gemileri Uzun Mesafeden Tanıma ve İzleme) ile izlenen gemilerden alınması beklenen datalar, koordinatlar, gemi bilgileri, mevcut pozisyon ve zaman bilgileri gibi verilerden oluşmaktadır [3]. **Şekil 2**'de bu sistemin mimarisi görülmektedir. LRIT ile VTMIS sistemleri

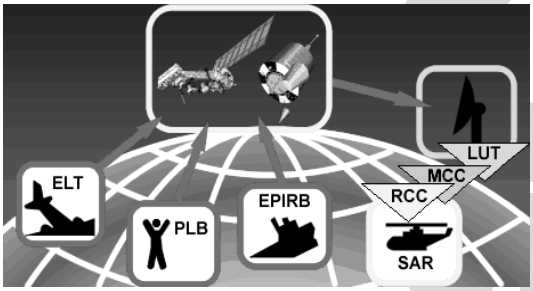
[1] İng. "Long Range Identification and Tracking of Ships"

arasındaki tek ve en önemli fark, VTMIS sistemlerinin broadcast mantıkla çalışması ve verici tarafından yayınlanan bilgilerin uygun alıcıları olan herkes tarafından alınabilme özelliğine sahip olması, LRIT de ise uluslararası kanunlarla belirlenmiş gizlilik çerçevesinde bilgi alınabilmesidir.



Şekil 2 LRIT Sistem Mimarisi

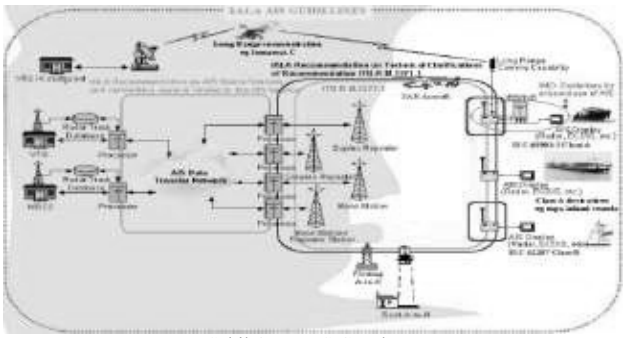
Arama Kurtarma maksatlı kullanılan COSPAS/SARSAT[2], acil durum anında mevkii ve ilgili diğer bilgiler, sorumlu COSPAS-SARSAT Görev Kontrol Merkezi (MCC[3]) tarafından Mahalli Kullanıcı Terminalleri (LUT[4]) vasıtası ile alınarak gerekli filtreleme işleminden sonra ilgili Arama ve Kurtarma yetkililerine gönderilir. **Şekil 3**'de genel yapısı verilen bu sistemin hedefi dünyanın neresinde olursa olsun denizde, karada veya havada Arama ve Kurtarma harekatından sorumlu kuruluşları desteklemektir [4].



Şekil 3 COSPAS/SARSAT Genel Yapısı

Arama Kurtarma modüllerinin yer aldığı Leo ve Geo uydularının algıladığı 406 Megahertz (MHz) veya 121.5-243 MHz'de çalışan imdat vericilerinden[5] alınan sinyallerin COSPAS-SARSAT ağı içerisinde yer alan ülkelerde kurulu görev merkezlerine (MCC) gönderilmesi sonucunda acil müdahale imkanı ve kurtarma çalışmalarına en kısa sürede başlanması imkanı sağlamaktadır.

Son olarak bahsedeceğimiz VTMIS, günümüzde dünyadaki birçok büyük limanda kullanılan modern sistemlerdendir [1]. Bu sistemlerin amacı özellikle, denizde seyir halinde olan veya olmayan deniz araçlarından bilgi sağlamak ve deniz trafiğini bu bilgiler ışığında yönlendirmek, temin edilen bu bilgileri gerekli yerlere iletmek, denizde bulunan araçlara seyir konusunda ve diğer aktivitelerinde yardımcı olmaktır. Bununla birlikte, **Şekil 4**'de yapısı gösterilen bu sistemlerin en büyük faydalarından biri de, deniz güvenliğini sağlamak, çevre kirliliğini engellemek ve deniz ulaşım yollarını etkin şekilde kullanımını sağlamaktır.



Şekil 4 VTMIS Genel Yapısı

VTMIS sistemleri, radar, digital veya taranmış haritalar ve çeşitli sensörlerden oluşmaktadır. Sistem üzerinde, deniz trafiğinin çok yoğun ve karışık olduğu yerlerde mevcut trafiği kolay bir şekilde nasıl yönlendirmek gerektiği konusunda çalışmalar halen devam etmektedir [4].

III. UYDU TABANLI SİSTEMLERDE BİLGİ İLETİŞİMİ ve GÜVENLİK

Yukarıda bahsedilen VTMIS sistemlerde denizde bulunan araçlardan gelen statik ve dinamik bilgilerin formatı IALA standartlarındadır. Ancak sivil gemilerle yapılan haberleşme bilgileri herhangi bir şifrelemeye tabi tutulmamaktadır. Bu nedenle VHF bandında haberleşme yapan sivil gemilerin gerek lokasyonları gerekse diğer bilgileri kolaylıkla izlenebilir yapıdadır. Benzer şekilde, COSPAS/SARSAT sistemlerinde ise ana amacın insan hayatının kurtarılması düşüncesi olması nedeni ile SAR uydularından alınan bilgilerin şifreleme uygulaması ülkemizde bulunmamaktadır.

Uygun techizata sahip olunması halinde yukarıda belirtilen sistemlerden kolaylıkla bilgi transferi yapılabilmektedir. Geçmişte bu tür olayların tecrübesi yaşanmış olup ülkemizin stratejik bilgilerinin kötü amaçlarla kullanımı, sözkonusu iletişim bilgilerinin güvenliğinin sağlanmasını zorunlu hale getirmiştir.

Son dönemlerde deniz trafiğini kontrol altına alma amaçlı olarak çeşitli kurumlarca denizcilik sektörüne yapılan yatırımlar sonucunda oluşturulan merkezlere iletilen bilgiler, söz konusu sistemlerin VHF bandında çalışması ve gemilerden iletilen bilgilerin karasal alıcılar tarafından alınması ve şifrelenmemiş olması nedeni ile yurt dışından ithal edilen ve kaçak olarak kullanılan alıcılar[6] vasıtası ile alınarak başka amaçlar için kullanılmıştır. Söz konusu vericilerin kötü amaçlı kişilerce kullanılması sonucu, insan ve mal kaçakçılığı, stratejik amaçlarla kullanım, kontrolsüz veri dağılımı gibi olaylarda kullanılarak deniz trafiğini her an tehlike altına sokacak durumu ortaya çıkmıştır. Öte yandan savaş ve benzeri

[2] Rus./İng. "Cosmicheskaya Sistyema Poiska Avariynich Sudov/ Search And Rescue Satellite-Aided Tracking"
[3] İng. "Mission Control Center"
[4] İng. "Local User Terminal"
[5] İng. "beacon"
[6] İng. "Transponder"

olağanüstü durumlarda da arama kurtarma verilerinin kötü niyetli kişilerce kullanımı engellenmelidir. Bu nedenle denizcilik sektöründe uydu tabanlı bilgi iletişiminde de şifreleme kullanılmalıdır.

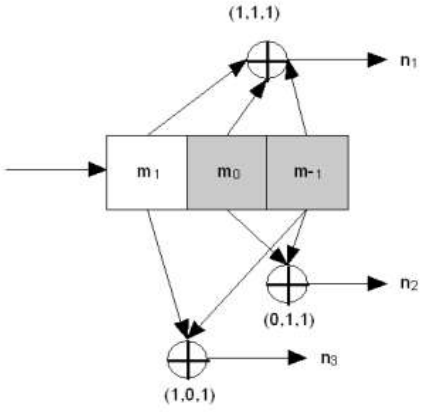
Gürültüden az etkilenen, ilgili frekans bandlarında uygulanabilen, hata oranı düşük, analog-dijital çevirimlerde probleme neden olmayan kodlama teknikleri ve hızlı şifreleme yöntemleri kullanıldığı takdirde sistemin amaçlarına uygun olarak bilgi güvenliği de sağlanmış olacaktır. Konvolüsyonel Kodlama arama kurtarma sinyallerindeki olasi hataları düzeltirken RSA şifreleme yardımıyla da bilgi güvenliği gerçekleştirilmiş olacaktır.

IV. KONVOLÜSYONEL KODLAMA ve RSA ŞİFRELEME

Telekomünikasyon alanında kullanılan konvolüsyonel kodlama[7], basitce m-bit uzunluğundaki bir verinin daha uzun olan n-bit uzunluğundaki bir veriye dönüştürülmesi yoluyla hata sinyal hatası düzeltme olarak görülebilir [5], [6]. Bu kodlamada m/n kod oranını verir ve k bilgi sembollerinin kullanıldığı bir transformasyon fonksiyonu vardır.

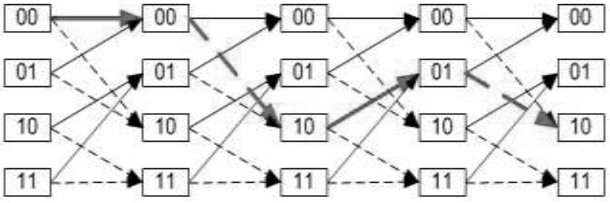
Konvolüsyonel kodlamada her biri 1 bit tutabilen k adet hafiza kayıtçıları vardır. Tüm bitlerin sıfırlanması ile başlayan kodlama işleminde, n modulo-2 toplayıcılar ve n üretici polinomlar kullanılır. Başlangıçta bir m_1 biti en sol kayıtçıya yerleştirilir. Daha sonra üretici polinomların ve diğer kayıtçılardaki mevcut değerlerin yardımıyla kodlayıcı n bit üretir. Ardından kayıtçılardaki bütün bitler sağa kaydırılarak bir sonraki m girdisi beklenir. Eğer herhangi bir girdi olmazsa kodlayıcı bütün bitleri sıfırlanana kadar çıktı üretmeye devam eder.

Şekil 5'de 1/3 kod oranı oranına sahip k=3 olan ve G_1 = (1,1,1), G_2 = (0,1,1), G_3 = (1,0,1) üretici polinomlarını kullanan örnek bir konvolüsyonel kodlama gösterilmiştir.



Şekil 5 Örnek Konvolüsyonel Kodlama (m/n=1/3, k=3)

Bu örneğe göre modulo-2 ile hesaplanan çıktı bitleri $n_1 = m_1 + m_0 + m_{-1}$, $n_2 = m_0 + m_{-1}$, $n_3 = m_1 + m_{-1}$ olacaktır. Konvolüsyonel kodlayıcı aslında bir sonlu durumlu makinedir[8]. Şekil 5'e ait olası tüm çıktı bitlerden oluşturulacak bir diyagram Şekil 6'daki trellis diyagramı ile gösterilmiştir. Bu diyagramdaki her bir dizi için Hamming Farkı hesaplanırsa ($t=\lfloor (d-1)/2 \rfloor$) gelen sinyaldeki olası hataların tespiti ve düzeltilmesi sağlanabilir. Kodlamanın çözülmesi için Viterbi Algoritması kullanılabilir [7].



Şekil 6 Olası Çıktı Durumları (Trellis Diyagramı)

Konvolüsyonel kodlama analog-dijital sistemlere uygun, gürültüden az etkilenen, mevcut frekans bantlarında çalışabilen, hızlı ve verimli bir kodlama tekniğidir. Konvolüsyonel kodlama ve Viterbi Algoritması yardımıyla iletilen ve olası hataları düzeltilen arama kurtarma uydu verilerinin RSA şifrelemesi yardımıyla güvenliği de sağlanmış olur.

A. RSA Şifreleme

1983 Yılında MIT'de geliştirilen RSA Şifreleme Algoritması açık anahtarlı bir şifreleme yöntemi olup oldukça güvenlidir. Öncelikle P ve Q gibi iki çok büyük asal sayı seçilir, Şekilde gösterildiği gibi öncelikle p ve q. Bunların birbirleriyle çarpılmasıyla n=p*q 'dan n elde edilir. Daha sonra (p-1)*(q-1) sayısıyla 1 dışında herhangi bir ortak böleni bulunmayan ve n'den küçük bir e sayısı seçilir. ve (e*d=1) sayısının (p-1)*(q-1) çarpımına tam olarak bölünmesini sağlayan bir d sayısı bulunur. Burada e açık, d ise gizlidir. Açık anahtarı (n,E) çifti, gizli anahtarı ise (n,D) çifti oluşturur. Gizli anahtar olan D sayısının (n,E) sayılarından elde edilmesi zor bir işlemdir. RSA sisteminin güvenliği çarpanlarına ayırma probleminin zorluğu temeline dayanır [8]. Bir x verisinin şifreli hali $y=x^n$ mod E olacaktır. Şifreli veriyi çözmek için $x = y^n$ mod D kullanılacaktır.

RSA Şifrelenmiş uydu verileri konvolüsyonel kodlama ile kodlandıktan sonra alıcılara iletilirse, Viterbi Algoritması yardımıyla olası hatalar düzeltildikten sonra şifrenin çözülmesi yapılırsa uygun bir hata düzeltme ve şifreleme kombinasyonu yapılmış olacaktır.

V. SONUÇ

Denizcilik sektörü ve arama kurtarma, uydu iletişiminin önemli olduğu bir alandır. INMARSAT, LRIT, COSPAS/SARSAT ve VTMIS gibi sistemler insan hayatı için en hızlı ve uygun arama kurtarma etkinliği sağlamakla birlikte deniz trafiğinin en verimli şekilde yönlendirilmesi içinde kullanılmaktadırlar. Ancak arama kurtarma kapsamında dahi olsa uydu verilerinin savaş ve benzeri durumlarda gizlilik derecesi olmalıdır. Öte yandan bu uydulardan alınan bilgilerin stratejik önemi de olup şifrelenmediği takdirde kaçakçılık ve casusluk gibi kötü amaçlar için de kullanılma riski mevcut ve

[7] İng. "Convolutional Coding"

[8] İng. "Finite State Machine"

çok yüksektir. Konvolüsyonel kodlama, hayati değeri olan bu verilerde olası sinyal hatalarını düzeltirken RSA şifreleme yardımıyla aynı verinin güvenliği sağlanmış olacaktır. Önerilen bu kombinasyon, hız ve verimlilik itibariyle mevcut sistemlere fazla yük getirmeyeceği gibi stratejik bilgilerin korunmasına da katkıda bulunacaktır.

KAYNAKLAR

[1] Chang, S. (2003). Vessel Identification and Monitoring Systems for Maritime Security. *Proceedings of 37th Annual IEEE International Carnahan Conference on Security Technology* (pp. 66-70). IEEE.
[2] (n.a.) This is inmarsat. (n.d.). Retrieved on 20 Aug. 2007 from http://www.inmarsat.com
[3] (n.a.) Maritime Security, (n.d.). Retrieved on 28 Aug. 2007 from http://www.imo.org/Safety/mainframe.asp?topic_id=905
[4] Levesque, D. (1993). The COSPAS/SARSAT System. *Proceedings of IEE Colloquium on Satellite Distress and Safety Systems* (pp. 3/1 - 3/4). IEEE.
[5] Couch, L.W. (1990). Digital and Analog Communication Systems. New York: Macmillan Publishing Campany.
[6] Pretzel, O. (1996). Error-Correcting Codes and Finite Fields. Oxford: Clarendon Press.
[7] Langton, C. (n.d.). Coding and Decoding with Convolutional Codes. Retrieved on 1 Sep. 2007 from http://complextoreal.com/chapters/convo.pdf
[8] Schneider, B. (1996) .Applied Cryptography. New York: John Wiley & Sons, Inc.