# Sivil Havacılık Siber Güvenliği Üzerine Bilimsel Makale

# Sivil Havacılık Siber Güvenliği Üzerine Bilimsel Makale: Kritik Uçuş Sistemlerine Yönelik Spoofing Saldırıları ve Alınması Gereken Önlemler  
  
## Özet  
Bu çalışma, sivil havacılıkta kullanılan kritik seyrüsefer sistemlerine yönelik spoofing saldırılarının etkilerini ve bu tehditlerle başa çıkmak için uygulanabilecek güvenlik önlemlerini incelemektedir. ILS, GNSS ve ACAS/TCAS sistemleri gibi temel sistemlerin spoofing saldırılarına karşı kırılganlıkları analiz edilmekte, ayrıca iletişim kesintilerine yol açan saldırılar detaylandırılmaktadır. Son olarak, daha güvenli protokollerin geliştirilmesi için öneriler sunulmaktadır.  
  
## Giriş  
Havacılık sektörü, yüksek güvenlik standartlarına bağlı kalarak yolcu ve yük taşımacılığında dünya çapında emniyet sağlamaktadır. Ancak modern uçuş sistemlerinin büyük bir kısmı radyo frekansları ve dijital iletişim protokollerine dayandığından, bu sistemler çeşitli siber tehditlere karşı savunmasızdır. Bu makalede, özellikle spoofing saldırıları üzerinde durularak seyrüsefer sistemlerinin manipüle edilmesinin doğurabileceği riskler ele alınmıştır.  
  
## ILS Spoofing Saldırıları  
### Tanım ve Etki  
Aletli İniş Sistemi (ILS), uçakların piste doğru yaklaşmalarını sağlamak için hassas sinyaller sağlar. Bir ILS spoofing saldırısı, bu sinyalleri sahte verilerle değiştirmek suretiyle uçağı yanlış bir yöne yönlendirebilir.  
  
### Saldırı Mekanizması  
ILS sisteminde saldırgan, yanlış localizer veya glide slope sinyalleri yayarak iniş açısını manipüle edebilir. Bu durum özellikle kötü hava koşullarında tehlikeli hale gelir.  
  
### Potansiyel Sonuçlar  
- Yanlış hizalanma.  
- Pistin dışına iniş veya iniş sırasında pistten çıkma riski.  
  
### Güvenlik Çözümleri  
- Sinyal şifreleme ve kimlik doğrulama mekanizmalarının entegrasyonu.  
- Redundant sistemlerin ve otonom doğrulama algoritmalarının kullanımı.  
  
## GNSS Spoofing Saldırıları  
### GNSS Sistemlerinin Önemi  
Küresel uydu navigasyon sistemleri (GNSS), GPS, GLONASS, Galileo ve Beidou gibi sistemleri içerir ve uçakların coğrafi konumlarını doğru bir şekilde belirlemelerini sağlar.  
  
### Spoofing Tehdidi  
Sahte GNSS sinyalleriyle uçak yanlış koordinatlara yönlendirilebilir. Saldırganlar, gerçek sinyalleri bastırarak veya kendi sahte sinyallerini yayınlayarak bu saldırıyı gerçekleştirir.  
  
### Güvenlik Çözümleri  
- Anten tabanlı çoklu sinyal algılama sistemleri.  
- GNSS alıcılarının şüpheli sinyalleri tanımlayabilmesi için sahte sinyal tespiti algoritmalarının geliştirilmesi.  
  
## ACAS/TCAS Spoofing Saldırıları  
### Tanım  
ACAS (Airborne Collision Avoidance System) veya TCAS (Traffic Collision Avoidance System), havada çarpışma önleme sistemleridir. Bu sistemler, pilotları potansiyel çarpışma tehditlerine karşı uyarır.  
  
### Spoofing Mekanizması  
Sahte trafik sinyalleri gönderilerek yanlış çarpışma uyarıları oluşturulabilir. Bu durum, otomatik pilotun devreden çıkmasına ve manuel müdahalenin zorunlu hale gelmesine yol açabilir.  
  
### Potansiyel Sonuçlar  
- Pilotların yanlış kararlar almasına neden olabilecek acil durum senaryoları.  
- Çarpışma riskinin artması.  
  
### Güvenlik Önlemleri  
- Veri bütünlüğü için şifreleme.  
- Sinyal tespit doğrulama sistemlerinin entegrasyonu.  
  
## İletişim Spoofing Saldırıları  
### Tanım ve Etki  
Uçuş sırasında kule ile iletişim hayati öneme sahiptir. Spoofing saldırıları, pilotlara yanlış yönlendirme sinyalleri iletebilir veya iletişim frekanslarını kesintiye uğratabilir.  
  
### Potansiyel Tehlikeler  
- Hatalı iniş talimatları.  
- Diğer uçaklarla koordinasyon eksikliği nedeniyle çarpışma riskleri.  
  
### Güvenlik Çözümleri  
- Frekans spektrumu analizine dayalı sahte sinyal tespit sistemleri.  
- İki yönlü kimlik doğrulama protokollerinin kullanımı.  
  
## Tartışma ve Sonuç  
Modern uçak sistemlerinde güvenlik açıkları, operasyonel emniyeti riske atmaktadır. Spoofing saldırıları, bu açıkların en tehlikeli örneklerindendir. Daha güçlü güvenlik protokollerinin uygulanması ve mevcut sistemlerin dayanıklılığının artırılması, bu tür tehditlere karşı kritik önlemler sağlayacaktır. Gelecekteki araştırmalar, siber saldırılara daha dirençli seyrüsefer ve iletişim teknolojilerinin geliştirilmesine odaklanmalıdır.