SAVTEK 2022, 10. SAVUNMA TEKNOLOJİLERİ KONGRESİ
13-15 Eylül 2022, ODTÜ, Ankara

GÜÇ SPEKTRAL YOĞUNLUĞU KULLANARAK SAHTE GPS SİNYALİ TESPİTİ

Mustafa TANIŞ [(a)], Can BOZACI [(b)], Seçkin GEZER [(c)] , Ramazan YENİÇERİ [(d)], Müştak Erhan YALÇIN [(e)]

[(a)] Araştırma Görevlisi, İTÜ Elektronik ve Haberleşme Müh. Bölümü, İstanbul, mtanis@itu.edu.tr

[(b)] Lisans Öğrencisi, İTÜ Elektronik ve Haberleşme Müh. Bölümü, İstanbul, bozacican@gmail.com

[(c)] Lisans Öğrencisi, İTÜ Elektronik ve Haberleşme Müh. Bölümü, İstanbul, seckingezerr@gmail.com

[(d)] Doktor Öğretim Üyesi, İTÜ Uçak Müh. Bölümü, İstanbul, yenicerir@itu.edu.tr

[(e)] Prof.Dr., İTÜ Elektronik ve Haberleşme Müh. Bölümü, İstanbul, mustak.yalcin@itu.edu.tr

ÖZET

Bu çalışmada bir yazılım tabanlı radyo verici (SDR) yardımıyla sahte GPS yayının yapılabildiği ve GPS alıcısının aldatılabildiği deneysel olarak gösterilmiştir. Aldatmaya karşı yüksek frekanslı RF sinyallerini ara frekansa düşürüp örnekleyen bir çevirici yardımıyla elde edinen sinyallerin güç spektral yoğunluğu üzerinden bir yöntem önerilmiş ve gerçekleştirilmiştir. Aldanmayı kısa zamanda fark edebilmek amacıyla çeviriciye bağlı sahada programlanabilir kapı dizilerinden faydalanılmıştır.
Anahtar Kelimeler: GPS, Sahte GPS Yayını, Sahte GPS Tespiti, Yazılım Tabanlı Radyo

ABSTRACT

In this study, it has been experimentally demonstrated that fake GPS broadcasts can be made and the GPS receiver can be deceived with the help of a software-based radio transmitter (SDR). Against GPS spoofing, a method is proposed and implemented based on the power spectral density of the signals obtained with the help of a converter that samples the high-frequency RF signals to an intermediate frequency. In order to realize the spoofing in a short time, field programmable gate series connected to the converter were used.
Keywords: Global Positioning System (GPS), GPS Spoofing, Antispoofing Technique, Software Defined Radio (SDR)

1. GİRİŞ

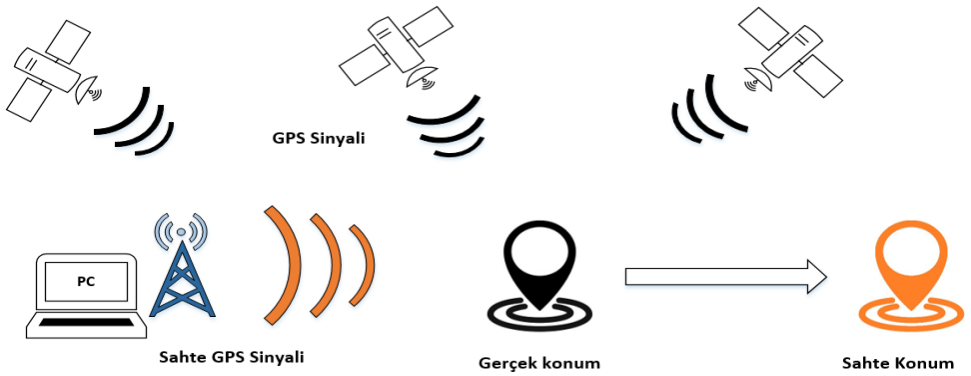
Gezinme (Navigasyon), bir insanı veya aracı bir yerden başka bir yere yönelimi olarak tanımlanmaktadır. Günlük yaşantımızda çeşitli gezinmeleri gerekli kılmaktadır. İşe arabayla gitmek veya bir mağazaya yürümek temel gezinim becerileri gerektirir. Birçoğumuz bu eylemi gerçekleştirirken duyu organlarımıza ve bazı işaretlere ihtiyaç duyarız. Günümüz dünyasında bu eylem için artık daha fazlasına ihtiyaç duymaktayız.

Bu ihtiyacı karşılamak üzere 1970'lerde Amerikan Savunma Bakanlığı kararlı ve dayanıklı bir uydu navigasyon sisteminin temellerini attı. 1978'de NAVSTAR adlı uydusuyla ilk navigasyon sistemini başlattı. 24 adet uydu sistemi ile 1993'te tamamen faaliyete geçildi. Bugün GPS, ABD hükümetinin sahip olduğu ve Amerikan Hava Kuvvetleri tarafından işletilen 32 uydu, çok kullanımlı, ulusal savunma, sivil, ticari ve bilimsel ihtiyaçları karşılamak için kullanılan bir radyo navigasyon sistemidir.

GPS verisi, cep telefonları, mobil robotlar, taşımacılık sektörü, savunma sanayi, ülke borsaları, akıllı sistemler ve hatta suçlu takibi uygulamalarında kullanılıyor olması bu verinin güvenliğinin ne kadar kritik bir öneme sahip olduğunu göstermektedir.

Yeryüzüne ulaşan GPS sinyallerin gücü yaklaşık -160dBw (1x10-16 watts) değerindedir. Bu da 25W'lık bir lambanın 15.000 km uzaktan görülmesine benzetilebilir[1]. Bu zayıf sinyal kolaylıkla engellenebilir veya benzer frekansta daha güçlü bir sinyal ile bastırılabilir. Sahte GPS saldırısını gerçekleştirmek için gerçek GPS sinyalinden daha güçlü bir sinyal yayınlanması gerekir. GPS alıcısı sahte sinyali uydudan gelen gerçek sinyal olarak değerlendirir ve gerçek sinyali yok sayar. GPS alıcısı bu yanlış yönlendirme sinyaline dayalı olarak hatalı konum veya zaman bilgisi hesaplamaya devam eder. Alıcı doğru olduğu düşünülen veriler ile işlem yapılması durumunda geri döndürülemez hatalara ortaya çıkabilir.

GPS verilerinin taklit edilmesi askeri alanda rekabet eden ülkeler veya ülkeler ile savaşan terörist grupların yaygın olarak kullandığı bir yöntem olmuştur.2011 yılında İran askeri güçleri tarafından Amerikan Hava Kuvvetlerine ait RQ-170 tipi bir insansız hava aracı herhangi bir zarar verilmeden GPS sinyalinin yönlendirilmesi ile ele geçirilmiştir[2]. 2012 yılında bu insansız hava aracının nasıl ele geçirildiği bilgisi kamuoyu ile paylaşılmıştır[3]. Ayrıca 2017 yılında Karadeniz'de bulunan bir tanker gemisinin navigasyon sistemi aniden olanaksız bir konumda olduğunu gösteriyordu. Geminin GPS alıcısı, gerçek konumu yerine 30 kilometre uzakta bir havalimanında olduğunu göstermekteydi. Daha sonrasında bu yanıltmanın Rus askeri kuvvetleri tarafından bir siber silah denemesi ile gerçekleştirildiği öne sürülmüştür[4].



Şekil 1: GPS Saldırı Modeli

Günümüz teknolojik seviyesinde, sistemleri engelleme yerine manipüle edebilme yeteneğine sahip olmak teknik açıdan daha kabiliyet gerektiren ve beklenen bir özellik haline gelmiştir.

Uydu konumları ve sinyalin yayılma süresi konumlamada iki önemli bileşen olduğundan, hedef GPS sinyali üretmenin bir yöntemi efemeris verilerinin manipüle edilerek sahte uydu konumları sağlamaktır veya sinyalin yayılma süresine gecikmeler ekleyerek kaydırmaktır.

Bu konuda yapılan başarılı çalışma incelendiğinde, sinyal gücünün ve gecikmesinin kademeli olarak değiştirilmesi ile saldırı altında olan alıcının başarılı bir şekilde manipüle edilebildiğini gösteren çalışmalara rastlanmaktadır[5]. Sahte GPS sinyali kodlarının alıcı tarafına belirli gecikmeler ile iletilmesi, alıcı üzerindeki etkilerini ve bunların alıcının hangi bloklarında etkilerinin incelenmesi yazılım tabanlı olarak değerlendirilmiştir[6]. Son yıllarda yazılım tabanlı radyo verici (SDR) gelişmesi ile sahte GPS yayının düşük maliyetli ve başarılı çalışmalarını literatürde görmekteyiz[7][8][9]. Açık kaynak verilerin kullanımı ile yapılan bu saldırılar çoğu kullanıcıyı tehdit eder durumdadır.

Sahte GPS sinyali saldırısının tespiti, GPS verisinin önemi ve bu saldırılar altında oluşabilecek zararlı etkiler göz önüne alındığında büyük önem kazanmaktadır. Mevcut saldırı tespit yöntemleri üç ana bölümde incelenebilir. İlk olarak yardımcı donanımlar ve bilgiler kullanmak, sinyal istatistiklerinden eşik oluşturmak, son olarak da kriptografik yöntemler ile kimlik doğrulama yöntemleri mevcuttur. Birden fazla alıcı kullanımı, anten çözümleri, gürültü sensörleri, atalet ölçer veya internet kullanılarak konum iyileştirme ve saldırı tespitleri yapılmaktadır[10][11][12][13].

2. SİSTEM MODELİ

GPS uyduları, L1 1575.42 MHz, L2 1227.6 MHz, L5 1176 MHz gibi birden fazla taşıyıcı frekansı üzerinden yayın yapmaktadır. Çalışma içerisinde sivil kullanıma uygun L1 bandı üzerine çalışılmıştır.

Oluşturulan test ortamına ilişkin diyagram şekil-2'de gösterilmiştir. Sistem, alıcı ve verici olarak iki ana bölümden oluşmaktadır. Alıcı, uydu üzerinden alınan bir gerçek GPS yayının yanında, SDR kullanılarak gerçekleştirilen 1575.42 MHz'de sahte GPS yayını saldırısı altında çalışmaktadır. Alıcı sistemine ulaşan sinyal sahte ve gerçek GPS yayının karışımıdır.

x_r, uydulardan gelen gerçek sinyali,H_r kanal çarpan değerini, η_r ise beyaz Gaussian gürültüyü olmak üzere, alıcıya uydudan ulaşan sinyal şeklinde ifade edilebilir.

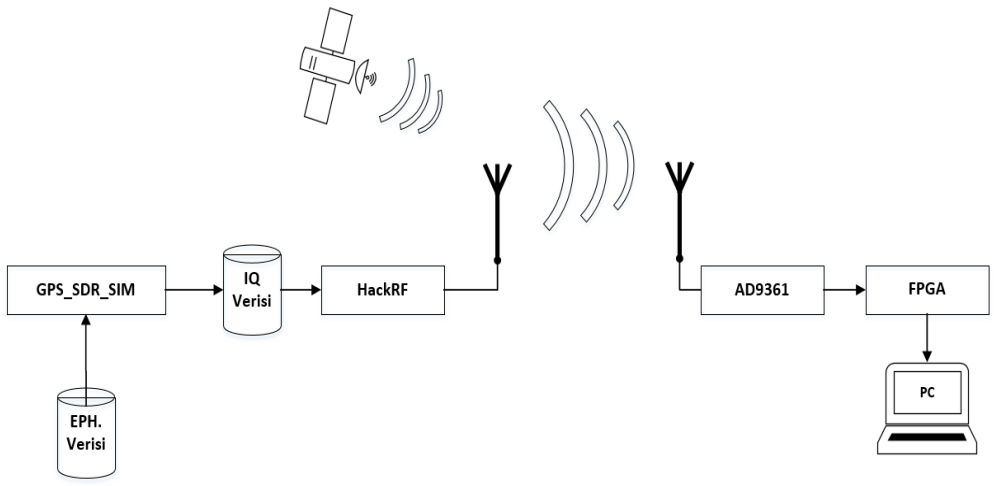
$$y_r = x_r * H_r + \eta_r \quad (1)$$

Benzer şekilde saldırıyı gerçekleştiren SDR sinyalinden alıcıya ulaşan sinyalin matematiksel modeli olarak ifade edilebilir.

$$y_s = x_s * H_s + \eta_s \quad (2)$$

Alıcı, saldırı sinyalinin güçlü etkisi nedeniyle gerçek GPS sinyalinden ayrılarak sahte sinyali takip edecektir.

Bu çalışmada, belirli zaman periyodu ile farklı boyutlarda pencereler kullanarak alıcıdaki sinyalin kendisi yerine güç spektral yoğunluğunu (PSD) (Power Spectral Density) inceleyerek saldırı tespiti yapılacaktır.

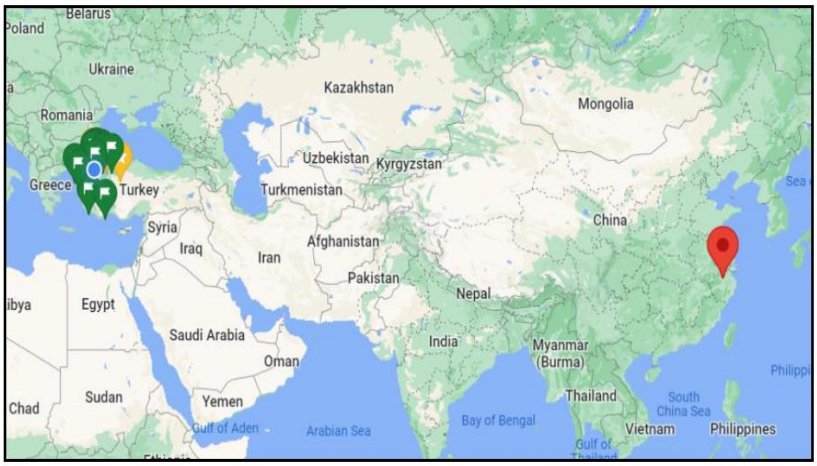


Şekil 2: Çalışmadaki GPS saldırı ve tespit sistemine ilişkin test düzeneğinin blok diyagramı

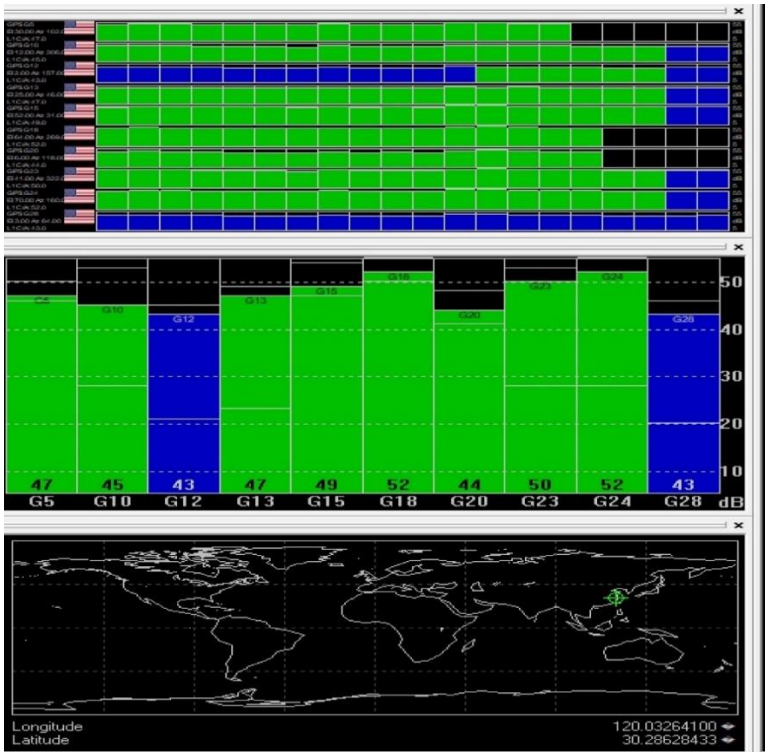
Örneğin, alıcıya ulaşan sinyal $\{y(t), y(t+1), \dots y(t+T-1)\}$ olarak ifade edersek, t şimdiki zamanı, T ise pencere boyutunu ifade etmektedir. Alınan sinyallerin spektral güç yoğunlukları $\{P_0, P_1, \dots, P_{T-1}\}$ olarak ifade edilir. Hesaplanan PSD değerlerini pencere boyutunda matris olarak ifadesi $S_t = [P_0, P_1, \dots, P_{T-1}]^T$ olacaktır. Elde edilen S_t matrisi ile bir önceki S_{t-1} matrisini literatürde iyi bilinen Runs testi ile karşılaştırarak rastgele dağılımın bozulduğunun tespiti amaçlanmıştır[14]. Runs testinin iki adet hipotezi mevcuttur. H_0 , hipotezi S_t matrisinin rastgele olduğunu söylerken, aksi hipotez bunu reddeder. Çalışmada H_0 , hipotezinin sağlanması herhangi bir saldırı olmadığını, aksi durumun alıcının saldırı altında olduğunu ifade etmektedir. İki pencerenin PSD'deki örnekler bağımsız ve aynı dağılımdan alındığından, Runs testinin amacı, dağılımlarının tutarlı olup olmadığının kontrol etmektir.

3. TEST ORTAMI VE ÇALIŞMASI

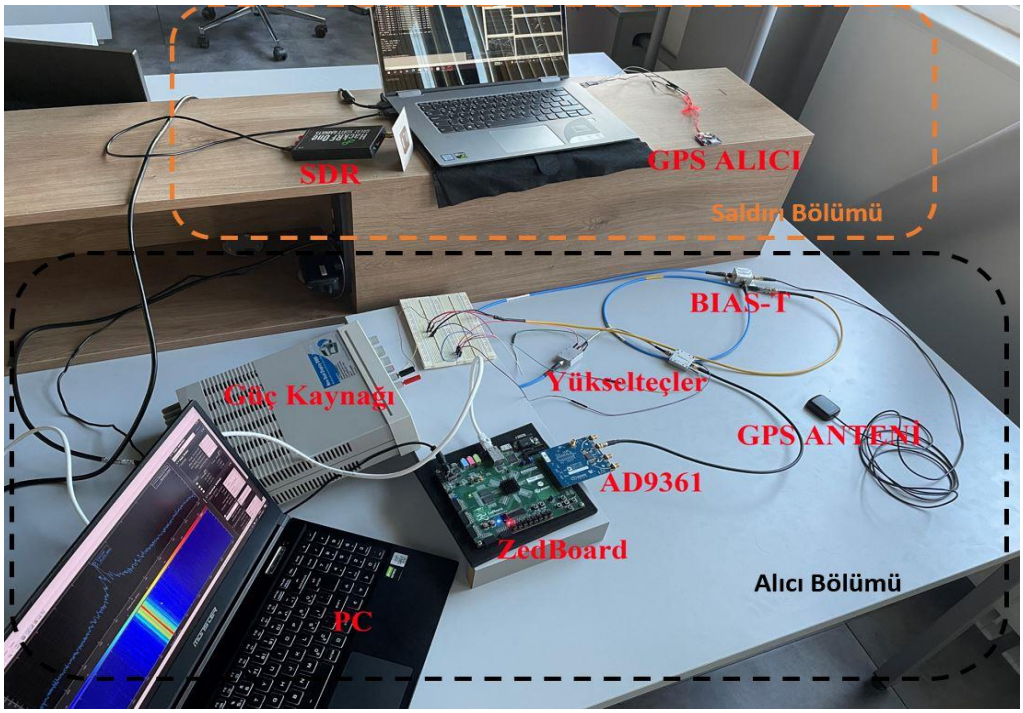
Bu çalışmada ilk olarak SDR üzerinden yapılacak yayın ile GPS alıcısının aldatılması üzerine yoğunlaşılmıştır. GPS_SDR_SIM açık kaynak kodlu yazılım ile istenilen enlem ve boylam konumunda U-blox Neo-6M GPS alıcısı üzerinde başarılı saldırılar gerçekleştirilmiştir[15].
Şekil-3'te görüldüğü üzere GPS alıcısı (30 17'11.4"N 120 01'57.6"E) koordinatına manipüle edilmesi amaçlanmıştır. Şekil-4'te GPS alıcısı U-center yazılımıyla gözlenerek, yapılan aldatıcı yayın GPS alıcısını başarılı şekilde aldatmıştır.



Şekil 3: Sahte GPS Saldırısı ile Yönlendirilmek İstenen Konum



Şekil 4: GPS Alıcısı Konum Bilgisi



Şekil 5: Deney Seti

Şekil-5'te görüldüğü üzere deney seti iki ana bloktan oluşmaktadır. İlk blok, sahte GPS yayının gerçekleştirildiği saldırı bölümü, diğer blok ise, aktif GPS anteni, yükselteç, güç kaynağı, AD9361 RF ön katmanı, Zedboard ve bilgisayardan oluşan alıcı bölümü olarak nitelendirilmiştir.
Saldırı bölümünde, sahte sinyal yayının L1 bandında 1575.42 MHz'de 2.6M örnekleme oranı ile 10 dB ve 20 dB kazanç faktörleri ile yayınlar yapılmıştır. Alıcı bölümünde ise Zedboard ile MATLAB Simulink arasında gerekli donanım/yazılım paketi konfigürasyonları sağlanarak iletişim sağlanmıştır. Alınan sinyallerin güç spektral yoğunlukları farklı çerçeve boyutları ile hesaplanarak değişimin tespiti amaçlanmıştır. Çerçeve boyutları, 32, 64, …,2048 ile ikinin katları ve FFT uzunluğu ile eşlenik olarak seçilmiştir. Her çerçeve için güç spektral yoğunluklar hesaplanarak bir önceki çerçeve değerleri için Runs testi uygulanmıştır. Farklı kazanç faktörü, pencere türleri ve çerçeve boyutları ile çizelge-1'deki sonuçlar elde edilmiştir. Runs testi ile güç spektral yoğunlukların rastgele olma eğilimin bozulduğunu bir önceki çerçeve ile karşılaştırılması yapılmış ve bu değişim bozulması ile sahte sinyal saldırısının tespiti arasında geçen sürede çizelge-1'de paylaşılmıştır.

Çizelge 1: Saldırı Tespiti Süre Analizi

Çerçeve Boyutları	Pencere Türleri			
	Hamming		Blackman	
	SDR Güçlendirmesi (dB)			
	10	20	10	20
	Sahte Sinyalinin Tespit Edilmesinde Geçen Süre (ms)			
32	0.24491	1.1	0.24491	1.1
64	1	1.7	1	1.7
128	1.92	3.1	1.92	3.1
256	6.3	6.2	6.3	6.2
512	11.9	12.2	11.9	12.2
1024	22.4	23.7	22.4	23.7
2048	43.8	46.9	43.8	46.9

Çizelge-1'den anlaşılacağı üzere, çerçeve boyutunun küçük seçilmesi, alınan örnek sayısının azaltıp, karşılaştırma ve karar mekanizmasını hızla yürütebildiği için sahte sinyal saldırısının sistem tarafında tespit edilmesi büyük çerçeve boyutlarına göre daha kısa sürede olmuştur.

3. SONUÇ

Bu çalışmada sahte GPS sinyali saldırısının SDR kullanılarak nasıl gerçekleştirildiği ve bu saldırılara yönelik gerçekleştirilen bir tespit tekniği anlatılmıştır. Sahte sinyalin başarılı bir şekilde GPS alıcısını aldatabildiği gösterilmiştir. Ek olarak sahte sinyal saldırılarının tespitine yönelik gerekli

donanımlar kullanılarak başarılı bir tespit yöntemi çalışılmıştır. Küçük çerçeveler alarak, sahte sinyal saldırısının tespiti 0.2 msn mertebesinde gerçekleştirilmiştir. AD9361'den gelen verilerin seçilen çerçeve boyutlarına uygun olarak alınıp güç spektral yoğunluğunun hesaplanması sırasında çerçeve boyutunun büyük olması anlık saldırının tespitini geciktirmektedir. Çerçeve boyutunun küçük olması ise karşılaştırılacak veri setini azaltacak ve daha hızlı karar mekanizmasını oluşturacaktır.

KAYNAKÇA

[1] J. S. Warner, R. G. Johnston, and Cpp Los Alamos, "GPS Spoofing Countermeasures," pp. 1296–1296, 2003.

[2] J. Reynolds, "URL-1." [Online]. Available: https://www.bbc.com/news/world-middle-east-16098562. [Accessed: 10-Dec-2020].

[3] F. Gardner, "URL-2," 2011. [Online]. Available: https://www.bbc.com/news/world-us-canada-16095823. [Accessed: 10-Dec-2020].

[4] D. Hambling, "URL-3." [Online]. Available: https://www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon/. [Accessed: 22-Dec-2020].

[5] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner, "Assessing the spoofing threat: Development of a portable gps civilian spoofer," 21st Int. Tech. Meet. Satell. Div. Inst. Navig. ION GNSS 2008, vol. 2, pp. 1198–1209, 2008.

[6] T. H. Kim, C. S. Sin, and S. Lee, "Analysis of effect of spoofing signal in GPS receiver," Int. Conf. Control. Autom. Syst., pp. 2083–2087, 2012.

[7] K. K. Songala, S. R. Ammana, H. C. Ramachandruni, and D. S. Achanta, "Simplistic Spoofing of GPS Enabled Smartphone," Proc. 2020 IEEE Int. Women Eng. Conf. Electr. Comput. Eng. WIECON-ECE 2020, pp. 460–463, 2020.

[8] H. Lin and Y. Qing, "GPS SPOOFING Low-cost GPS simulator," no. December, 2015.

[9] G. Blass, A. Hennigar, and S. Mao, "Implementation of a Software-Defined Radio based Global Positioning System Repeater," 2015 ASEE Southeast Sect. Conf., 2015.

[10] K. Jansen, N. O. Tippenhauer, and C. Pöpper, "Multi-receiver GPS spoofing detection," pp. 237–250, 2016.

[11] D. Borio and C. Gioia, "Real-time jamming detection using the sum-of-squares paradigm," Proc. 2015 Int. Conf. Localization GNSS, ICL-GNSS 2015, pp. 6–11, 2015.

[12] X. J. Cheng, J. N. Xu, K. J. Cao, and W. Jie, “An authenticity verification scheme based on hidden messages for current civilian GPS signals,” ICCIT 2009 - 4th Int. Conf. Comput. Sci. Converg. Inf. Technol., pp. 345–352, 2009.

[13] Y. Chang, “Fake GPS Defender : A Server-side Solution to Detect Fake GPS,” no. c, pp. 36–41, 2018.

[14] X. Wei, M. N. Aman, and B. Sikdar, “Light-weight GPS spoofing detection for synchrophasors in smart grids,” 9th IEEE Int. Conf. Power Electron. Drives Energy Syst. PEDES 2020, pp. 2020–2023, 2020.

[15] “URL-4.” [Online]. Available: https://github.com/osqzss/gps sdr sim. [Accessed: 23-Dec-2021].