Askeri Araçlar Arası Güvenli Görünür Işık ile İletişim Protokolü (SV^{2}LC)

Seyhan UÇAR [(a)], Sinem Çöleri ERGEN [(b)], Öznur ÖZKASAP[(c)], Mustafa ERGEN[(d)]

[(a)] Doktora Öğrencisi, Koç Üniversitesi, Bil. Müh. Böl., 34450, İstanbul, sucar@ku.edu.tr

[(b)] Doç. Dr. Koç Üniversitesi, Elek. ve Elekt. Müh. Böl., 34450, İstanbul, sergen@ku.edu.tr

[(c)] Doç. Dr. Koç Üniversitesi , Bil. Müh. Böl., 34450, İstanbul, oozkasap@ku.edu.tr

[(d)] Doç. Dr. Koç Üniversitesi, Elek. ve Elekt. Müh. Böl. 34450 / MiSONE Solution, İstanbul, mergen@ku.edu.tr

ÖZET

Tasarsız Taşıt Ağları (VANET) uygulama alanlarından bir tanesi de askeri tasarsız taşıt ağlarıdır. Askeri tasarsız taşıt ağlarında taşıtlar konvoy halinde hareket etmekte ve son derece güvenilir bağlantı gerektirmektedirler. Fakat VANET güvenlik saldırılarına açık olup, farklı alternatif iletişim teknolojilerine ihtiyaç duymaktadır. Öte yandan, Görünür Işık ile İletişim (VLC) yeni nesil iletişim teknolojilerinden olup, ışık doğrusal yönlülüğü özelliği ile olası güvenlik saldırılarından daha az etkilenmektedir. Fakat, ışık ile gönderilen verinin ışık kapsama alanı gizliliği hala önemli bir problemdir. Bu çalışmamızda, gizli bir anahtar ile verinin şifrelendiği ışık veri gönderim gizlilik protokolü (SV^{2}LC) üzerine yoğunlaşmaktayız. SV^{2}LC' de ışık doğrusal yönlülük özelliği ile sadece hedeflenen taşıtlar arası iletişim gerçeklenmektedir. Taşıtlar çift-yönlü, kızıl ötesi (IR) ile gizli anahtar ve VLC ile veri iletimi, olacak şekilde haberleşmektedirler. Önerilen protokol deneysel olarak dış ortam şartlarında, farklı taşıt uzaklıklarında, veri paketi teslim oranı ve gecikme süresi başarım ölçümleri dikkate alınarak test edilmiştir.

Anahtar Kelimeler: askeri tasarsız taşıt ağları, görünür ışık ile iletişim, güvenlik, veri gizliliği.

ABSTRACT

One application area of vehicular ad hoc network (VANET) is military services, namely military ad hoc network, where vehicles are traveling as a convoy and require an fully-reliable connection. However, VANETs is open to security attacks that necessitate alternative technologies. Visible Light Communication (VLC), on the other hand, is a new technology that has little influence on security attacks due to the directivity of light. However, vehicular VLC based confidentiality service is still open problems. In this paper, we are proposing a light confidentiality service (SV^{2}LC) for military communication where the secret key is used to encrypt data in light. We use directionality to ensure only target vehicle participate in communication. The vehicle uses full-duplex communication, infra-red (IR) to share a secret key and VLC to receive data. We experimentally evaluate the suitability of SV^{2}LC in outdoor scenarios in

varying distance with different key metrics of interest including data delivery ratio and delay.
Keywords: military ad-hoc network, visible light communication, security, data confidentiality.

1. GİRİŞ

Önemli iletişim teknolojilerinden olan Tasarsız Taşıt Ağları (VANET) Akıllı Taşıma (ITS) ve Akıllı Trafik (ITF) sistemleri ile hız kazanmış durumdadır. Günümüz ITS ve ITF sorunlarını çözmek adına VANET, gelecek vaat eden ümit verici bir teknolojidir. Mobil tasarsız ağ yapılarından olan VANET, taşıttan taşıta (V2V), taşıttan baz istasyonuna (V2I) veya melez [1] şekillerde iletişim sağlamaktadır. VANET uygulama alanlarından bir tanesi de askeri tasarsız ağ yapılarıdır. Askeri tasarsız ağ yapıları, zaman bölüşümlü kanal erişim kontrol protokolü kullanmakta olup, Amerika Savunma Bakanlığı açık araştırma çağrısı ile araştırma anlamında hız kazanmıştır. Kablosuz ağlardaki gelişmeler, askeri tasarsız ağ yapılarını olur kılmış ve bu alandaki çalışmaları araştırma boyutundan ticari uygulamalar boyutuna taşımıştır [2].

Askeri tasarsız taşıt ağlarında, taşıtlar yol boyunca konvoy şeklinde hareket etmekte ve periyodik olarak IEEE 802.11p protokolünü (DSRC) kullanarak birbirleri ile veri paylaşımı yapmaktadır. Askeri tasarsız taşıt ağlarındaki bu veri paylaşımı son derece güvenlik, yüksek veri hızı, kısa gecikme ve yüksek veri paketi teslim oranı gerektirmektedir. Buna ek olarak, askeri taşıt ağları gereksinimlerinden biri de gönderilen veri içeriğinin kapsama alanında bulunan taşıtlar tarafından başarılı bir şekilde alınmış olsa bile anlaşılmamasıdır. Sonuç olarak, askeri tasarsız taşıt ağları çok yüksek güvenlik gerektirmekte ve alternatif güvenli haberleşme tekniklerine ihtiyaç duymaktadır.

Öte yandan, gelişen kablosuz iletişim teknolojileri ve artan veri trafiği DSRC üzerinde radyo frekans kıtlığına neden olmuş ve bu teknolojiyi askeri tasarsız ağlar için yetersiz kılmıştır. Buna ek olarak, DSRC olası sinyal boğma ve taklit etme güvenlik saldırılarına olanak vermektedir. Kapsama alanında bulunan herhangi bir taşıt, askeri araçlar arası iletişimi boğma sinyali göndererek bloke edebilmektedir. Taklit etme saldırısında ise herhangi bir araç askeri araçlardan birinin kimliğini veri toplayarak ele geçirmekte ve askeri taşıtları hatalı veri gönderimi ile tehdit etmektedir. Diğer taraftan, radyo frekans kıtlığı araştırmacıları alternatif 5. nesil haberleşme teknolojileri araştırmaya itmiş ve bu iletişim şekillerinden biri VLC olmuştur.

5. nesil iletişim teknolojilerinden olan VLC gönderilmek istenen veriyi kiplemekte ve var olan ışık hücrelerini çok hızlı bir şekilde açıp kapatarak karşı tarafa aktarmaktadır. Son dönemlerde VLC araştırmacılar tarafından büyük ilgi görmüş ve kanal özellikleri [3-4], iletişim gereksinimleri [5-8], DSRC ile melez yapılarda uygunluk [9] gibi amaçlar doğrultusunda çalışılmıştır. Fakat, güvenlik içerimli VLC iletişimine yeteri kadar önem verilmemiş, güvenlik hedefli VLC araştırmalarına birkaç çalışmada [10-11] odaklanılmıştır. Fakat güvenlik içerimli bu VLC araştırmaları, taşıtlar arası haberleşmeyi hedeflemediği için, taşıtlar

arası güvenli iletişim açısından uygun değildir. Öte yandan, askeri taşıtlar arası, sadece askeri taşıtların veriyi çözümleyebildiği bir gönderim gizlilik protokolü, taşıtlar arası iletişim güvenliliği için her zaman bir gereksinim olmuştur.

Bu çalışmamızda, askeri taşıtlar arası iletişimin VLC ile yapıldığı, gizli bir anahtar ile verinin şifrelendiği ışık veri gönderim gizlilik protokolü (SV^2LC) üzerine yoğunlaşmaktayız. Askeri taşıtlar ön farları aracılığı ile sadece konvoy ön tarafında bulunan araçları iletişim için hedefleyecek, çift-yönlü, IR ile gizli anahtar ve VLC ile veri iletimi, olacak şekilde haberleşebileceklerdir. Oluşturduğumuz dış ortam deney senaryosu ile farklı taşıtlar arası uzaklıklarda, veri paketi teslim oranı ve gecikme süresi başarım ölçümleri dikkate alınarak SV^2LC protokol uygunluğu test edilmiştir. Anlatım planımız şu şekilde düzenlenmiştir. Bölüm II ' de DSRC ve VLC önemli özellikleri karşılaştırılmalı ele alınacaktır. Bölüm III' te kullanılan askeri taşıtlar arası deneysel sistemi sunulacaktır. Bölüm IV 'de önerilen askeri taşıtlar arası ışık veri gönderim gizlilik protokolü (SV^2LC) detaylı şekilde anlatılacak, Bölüm V' de SV^2LC başarım ölçümü incelenecektir. Bölüm VI' da var olan test sonuçları üzerinden sonuç değerlendirmesi yapılacaktır.

2. DSRC VE VLC KARŞILAŞTIRILMASI

VLC ve DSRC önemli özelliklerinin karşılaştırılması Tablo 1' de sunulmuştur. DSRC' ye karşın VLC, yön bağımsal, 25-50 metre arası kısa mesafelerde, düşük maliyet ve ücretsiz frekans bandında çalışmaktadır. Taşıtlar arası iletişim yöntemlerinden birinin VLC olması kaçınılmazdır. Çünkü, var olan bir çok taşıt VLC gönderim ünitesi LED lambaları farlarında, fren lambalarında ve alıcı ünite olan kameraları park amaçlı bünyesinde barındırmaktadır.

Tablo 1 DSRC ve VLC önemli özellikleri karşılaştırılması

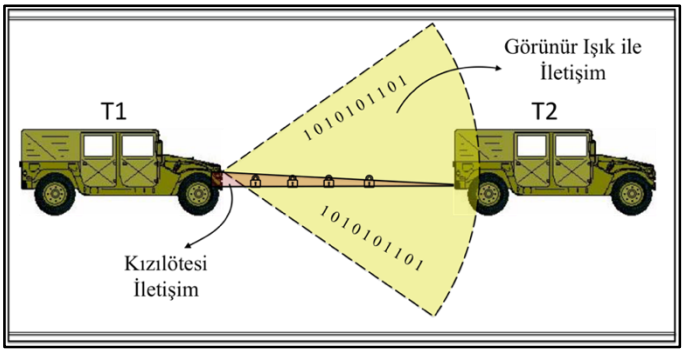
Özellik	**VLC**	**DSRC**
İletişim Senaryosu	Genellikle Doğrusal Görüş (LoS)	LoS ve Doğrusal olmayan Görüş (NLoS)
İletim Alanı	Kısa Erim ve Yön Bağımsal	Uzun Erim ve Genellikle Tümyönlü
Frekans Bandı	400 - 790 THz	5.8 - 5.9 GHz
Lisans	Ücretsiz	Gerekli
Kapsama Alanı	Dar	Geniş
Maliyet	Düşük	Yüksek
Hareketlilik Hassasiyeti	Orta	Yüksek
Hava Durumu Duyarlılık	Hassas	Dayanıklı
Ortam Işığı Hassasiyeti	Hassas	Etkilenmez

VLC sistemlerinde var olan LED lambalar insan gözünün fark edemeyeceği düzeyde hızlı bir şekilde açıp kapanarak gerek bina içi, gerekse bina dışı iletişim ve aydınlanma sağlanmaktadır. VLC, ışık doğrusal yönlülük ve dar alan özelliği ile olası güvenlik saldırılarından daha az etkilenmektedir. VLC güvenlik saldırısı, güçlü bir ışık kaynağının alıcı üniteye tutulması ile gerçekleştirilebilmektedir. DSRC de olası saldırıdan kapsama alanında bulunan tüm taşıtların etkilenmesine karşın, VLC' de sadece tek bir bağlantı etkilenmektedir. Bu

açıdan bakıldığı zaman, VLC olası taşıtlar arası güvenlik saldırılarını önleyebilmek adına umut verici bir iletişim teknolojisidir.

3. DENEYSEL SİSTEM

Askeri taşıtlar arası VLC deney sistemi Şekil 1' de gösterilmiştir. Deneysel sistem iki taşıt (T1 ve T2), ışık ile veri gönderimi için Li-1st [12] cihazı, Li-1st cihazına bağlı verici ünitesi (VU), foto diyot bazlı alıcı ünitesi (AU) ve iki adet LED sis lambasından oluşmaktadır. Çift simetrik LED lambaları, 36 cm yüksekliğinde aralarında 150 cm olacak şekilde tripodlara monte edilmiştir. Yapılan deneylerde otomobil sis lambalarının kullanılmasındaki sebep, sis lambalarının geniş görüş açısı özelliği ve yansımalara karşı dayanıklı yapıya sahip olmasıdır. Taşıt bilgi ve duyu verilerini içeren paketler iki taşıt LED sis lambalarının bağlı olduğu Li-1st VU ile gönderilmektedir. VU kiplenim olarak vurum (darbe) genlik kiplenimi (PAM), hata doğrulama tekniği olarak Reed-Solomon kodlamasını kullanmaktadır. Li-1st 4PAM ve mevcut diğer özellikleri ile 5Mbps'e kadar veri hızı sunmaktadır.



Şekil 1 Askeri Taşıtlar Arası VLC Sistem Modeli

Gerek AU, gerekse VU bilgisayarlara bağlı bulunmakta olup gönderilen ve alınan paketler başarım ölçüm amaçlı kaydedilmiştir. Güneş ışığı etkisini en aza indirmek amaçlı deney gece koşullarında gerçekleştirilmiştir. Tüm yapılan deneylerde, iki taşıt arası 100 paket Li-1st VU ve AU arasında gönderilmiş ve başarım ölçümleri gönderilen paketler üzerinden yapılmıştır.

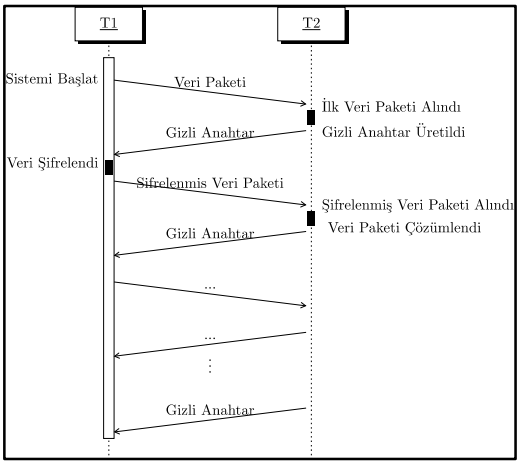
4. ASKERİ VERİ GÖNDERİM GİZLİLİK PROTOKOLÜ (SV^{2}LC)

Önerilen SV^{2}LC güvenli askeri taşıtlar arası görünür ışık ile iletişim protokolü özellikleri aşağıdaki gibidir;

1- Işık doğrusal yönlülüğü özelliği ile sadece hedeflenen askeri taşıtlar ile iletişim gerçekleşmektedir.
2- Şifrelenen verinin gizli anahtar olmaksızın çözümlenemediği, gizli anahtar oluşumu ve paylaşım mekanizması kullanmaktadır.
3- Eş zamanlı, IR ile gizli anahtar ve VLC ile şifrelenmiş veri iletiminin gerçeklendiği, çift yönlü olacak şekilde çalışmaktadır.

Şekil 2, SV^{2}LC protokolü aşamalarını göstermektedir. SV^{2}LC, beş aşamadan oluşmaktadır ve bunlar sırası ile; sistem başlatımı, gizli anahtar oluşturulması,

IR ile anahtar paylaşımı, veri şifrelenmesi/çözümlenmesi ve VLC ile şifrelenmiş verinin iletimi şeklindedir.



Şekil 2 SV^{2}LC protokol aşamaları

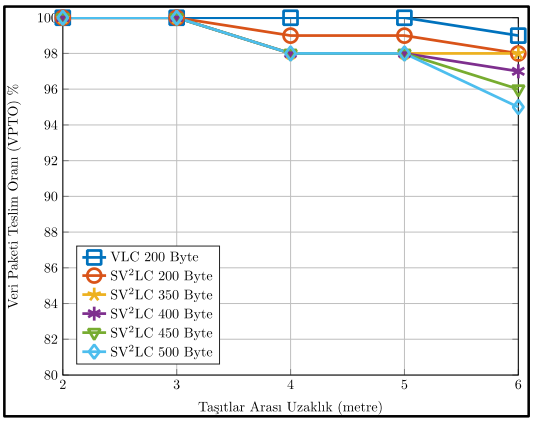
SV^{2}LC, sistem başlatımı ile gerekli donanımları hazır hale getirip, T2 'den gelecek gizli anahtarı beklemeye başlamaktadır. T2 ise alınan ilk veri paketi ile gizli anahtar oluşturmakta ve IR ile T1' e iletmektedir. Bu iletim şekli ile DSRC de kapsama alanında bulunan tüm taşıtların gizli anahtarı alabildiği senaryoya karşın, sadece T1 gizli anahtarı alabilmektedir. IR' in LoS özelliği bu tarz bir gönderimle dezavantaj olmaktan çıkıp, avantaja dönüşmüştür. Oluşturulan gizli anahtarlar, Gelişmiş Şifreleme Standardı (AES) kullanılarak üretilmektedir. AES, hızlı bakışımlı anahtar üretimi, diğer alternatiflere karşın daha güçlü olması ve henüz AES' e karşın uygulanabilir bir güvenlik saldırısı olmaması gibi özellikleri sebebi ile tercih edilmiştir.

Gizli anahtarın IR ile alınmasıyla T1, aktarılmak istenen veriyi alınan gizli anahtar ile şifreleyip ışık ile göndermektedir. Işık kapsama alanında herhangi bir taşıt olsa bile şifrelenmiş veri bu taşıtlar için bir anlam ifade etmemektedir. Verinin gizli anahtar olmaksızın anlamsız olması, DSRC bazlı önemli güvenlik problemi kulak misafiri olma sorununu çözmüştür.

5. BAŞARIM ÖLÇÜMÜ

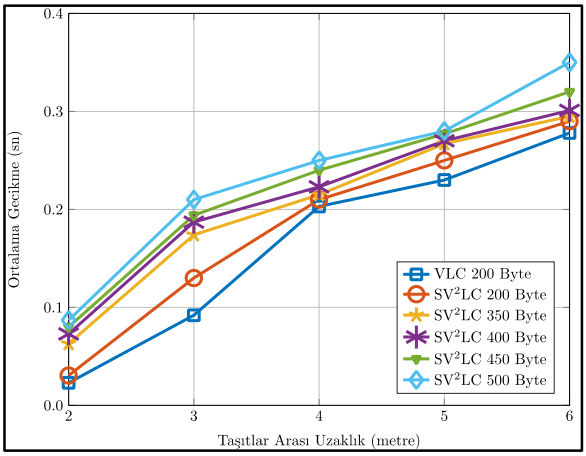
Önerilen SV^{2}LC protokolü, Java ile Li-1st cihazı üstünde, Keyczar [13] anahtar oluşturma aracı ile bütünleşik şekilde geliştirilmiştir. Keyczar, Google şirketi tarafından geliştirilmiş, kullanıcıların şifreleme ve çözümleme işlemlerini kolaylaştırmak için kullanılan bir araçtır. Li-1st, IR iletişim amaçlı iki adet Vishay [14] IR diyotu kullanmaktadır. Taşıtlar arası başarım ölçümlenmesi iki metrik üzerinden yapılmıştır. Bu metrikler, Veri Paketi Teslim Oranı (VPTO) ve gecikme süresi olarak belirlenmiştir. VPTO, her deneyde gönderilmiş olan 100 paketten kaçının Li-1st AU tarafından başarılı bir şekilde alındığını göstermektedir. Ortalama gecikme süresi, gönderilen paketlerdeki gecikme süreleri toplamının başarılı bir şekilde gönderilen paket sayısına bölünmesi ile hesaplanmaktadır. Öte yandan, maksimum gecikme süresi T1' den T2 'ye

gönderilmiş paketler arası en yüksek gecikme süresi değeridir. Karşılaştırma amaçlı, ışık ile iletişim iki taşıt arası gerçeklenmiş ve VLC olarak adlandırılmıştır. Paketlerin boyut büyüklüğünün SV²LC olan etkisi farklı paket boyutlarında deneyin gerçeklenmesi ile incelenmiştir.



Şekil 3 VPTO ölçüm karşılaştırması

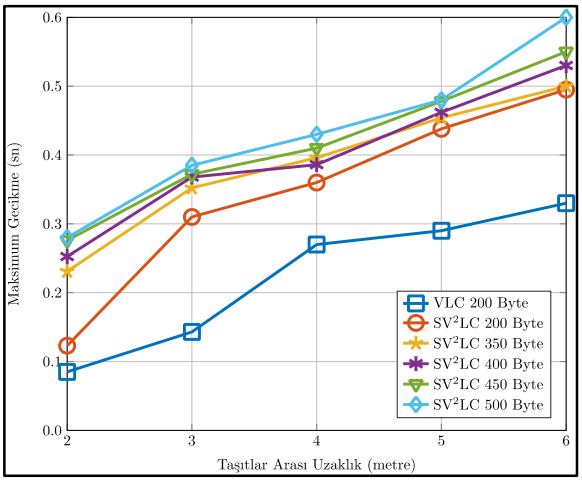
Farklı taşıtlar arası uzaklık ve farklı veri paketi boylarında ölçümlenen VPTO Şekil 3‘ te sunulmuştur. Yapılan karşılaştırılmalı ölçüm deneyi S²VLC ve VLC’ in aynı VPTO azalış modeline sahip olduğunu göstermiştir. Öte yandan, S²VLC’ de var olan VPTO azalma sebeplerinden birinin paylaşılamayan gizli anahtar olduğu anlaşılmıştır. Gizli anahtarın alınmadığı durumlarda, gönderilmek istenen veri anahtar ile şifrelenmediği için aktarılamamıştır.



Şekil 4 Ortalama gecikme süresi ölçüm karşılaştırması

Şekil 4’ de, SV²LC ve VLC ortalama gecikme süresi ölçüm deney sonuçları verilmiştir. Yapılan ortalama gecikme süresi analizi VLC’ ye karşın SV²LC’ nin daha fazla gecikme süresine sahip olduğunu göstermiştir. Bunun yanı sıra, artan paket boyutu şifreleme ve çözümleme aşamalarında var olan ortalama gecikme süresinde önemli rol oynamıştır. Paket boyutu arttıkça, SV²LC için

ortalama gecikme süresi artmıştır. VLC ile karşılaştırıldığında, SV^{2}LC, gizli anahtar üretimi, anahtar paylaşımı, veri şifrelenmesi ve veri çözümlenmesi işlemlerini içermektedir. Öte yandan, veri iletiminin VLC' ye kıyasla daha güvenli olduğu dikkate değer diğer bir noktadır. Bu noktadan hareketle, SV^{2}LC' de mevcut ortalama gecikme kabul edilebilir bir düzeydedir.



Şekil 5 Maksimum gecikme süresi ölçüm karşılaştırması

Taşıtlar arası SV^{2}LC ve VLC için ölçümlenen maksimum gecikme süreleri Şekil 5' de gösterilmiştir. Maksimum gecikme süresi analizi SV^{2}LC 'in VLC ye karşın daha yüksek gecikme süresine sahip olduğunu ortaya koymuştur. Paket büyüklüğü arttıkça, ölçümlenen maksimum gecikme süresi de bu yönde artmıştır. SV^{2}LC' de maksimum gecikme VLC' ye karşın yüksek olmasına rağmen, veri gizliliği ve güvenliği avantajları ile bu gecikme kabul edilebilir durumdadır.

6. VARGI

Taşıtlar arası iletişim uygulama alanlarından biri de askeri tasarsız taşıt ağlarıdır. Askeri taşıtlar arası iletişim alternatiflerinden birinin VLC olması kaçınılmazdır. Fakat, askeri taşıtlar arası iletişim güvenliği önemli gereksinimlerden biridir. Bu çalışmamızda, askeri taşıtlar arası iletişimin VLC ile gerçeklendiği güvenli iletişim protokolü, SV^{2}LC' ye odaklanmış bulunmaktayız. SV^{2}LC' de taşıtlar çift yönlü, IR ile gizli anahtar ve VLC ile veri iletimi, olacak şekilde haberleşmektedirler. Önerilen protokol SV^{2}LC, deneysel olarak veri paketi teslim oranı ve gecikme süresi başarım ölçüm metrikleri hesaba katılarak incelenmiş, uygunluğu test edilmiştir. Deneysel ölçümler, SV^{2}LC' nin VLC ye karşın daha yüksek gecikme süresine sahip olduğunu ortaya koymuştur. Fakat, veri gizliliği ve güvenli iletişim gereksinimleri dikkate alındığında SV^{2}LC askeri taşıtlar arası iletişim için uygundur.

KAYNAKÇA

[1] S. Ucar; S. Coleri Ergen; O. Ozkasap (2016), "Multi-Hop Cluster based IEEE 802.11p and LTE Hybrid Architecture for VANET Safety Message Dissemination," in Transactions on Vehicular Technology, IEEE.

[2] I. Rubin, A. Baiocchi, F. Cuomo and P. Salvo, (2013), "Vehicular Backbone Network Approach to Vehicular Military Ad Hoc Networks," Military Communications Conference, MILCOM, IEEE.

[3] W. Viriyasitavat, S. H. Yu and H. M. Tsai, (2013), "Short paper: Channel model for visible light communications using off-the-shelf scooter taillight," Vehicular Networking Conference (VNC), IEEE.

[4]P.Luo, Z. Ghassemlooy, H. L. Minh, E. Bentley, A. Burton, and X. Tang, (2015), "Performance analysis of a car to car visible light communication system," Appl. Optics.

[5] S. Ucar, B. Turan, S. Coleri Ergen, O. Ozkasap, and M. Ergen, (2016), "Dimming Support For Visible Light Communication in Intelligient Transportation and Traffic System," in Urban Mobility and Intelligient Transportation System (UMITS), IEEE.

[6] S. Ucar, S. Coleri Ergen, and O. Ozkasap, (2016), "Visible Light Communication in Vehicular Ad-Hoc Networks," in Signal Processing and Communication Application (SIU), IEEE.

[7] B. Turan, S. Ucar, S. Coleri Ergen, and O. Ozkasap, (2015), "Dual Channel Visible Light Communications for Enhanced Vehicular Connectivity," Vehicular Networking Conference (VNC), IEEE.

[8] H.-Y. Tseng, Y.-L. Wei, A.-L. Chen, H.-P. Wu, H. Hsu, and H.-M. Tsai, (2015), "Characterizing link asymmetry in vehicle-to-vehicle Visible Light Communications," in Vehicular Networking Conference (VNC), IEEE.

[9] S. Ishihara, R. V. Rabsatt, and M. Gerla, (2015), "Improving Reliability of Platooning Control Messages Using Radio and Visible Light Hybrid Communication," Vehicular Networking Conference (VNC), IEEE.

[10] A. Mostafa and L. Lampe, (2014), "Physical-layer security for indoor visible light communications," in International Communications Conference (ICC), IEEE.

[11] B. Zhang, K. Ren, G. Xing, X. Fu, and C. Wang, (2014), "SBVLC: Secure barcode-based visible light communication for smartphones," in INFOCOM, Proceedings IEEE.

[12] Li-1st, @Online: http://goo.gl/rAKqC4

[13] Keyczar, @Online: https://goo.gl/LMuY1I

[14] Vishay IR Diyot, @Online: http://goo.gl/2DIKcq