Araştırma Makalesi / Research Article

Otomotiv haberleşmesinde denetleyici alan ağı için hibrit bir saldırı savuşturma uygulaması

Serkan BAKİ[1]

Nedim TUTKUN[2]

Geliş tarihi / *Received*: 06.01.2021
Düzeltilerek geliş tarihi / *Received in revised form*: 19.02.2021
Kabul tarihi / *Accepted*: 23.02.2021

Öz

Teknoloji geliştikçe insanların yaşam kalitesinden beklentileri de her geçen gün artmaktadır. İnsanlar her alanda olduğu gibi otomotiv alanında da kaliteli yaşam sürmek istemektedir. Otomotiv teknolojisi insanların yaşam kalitesini artırmak için teknolojisini her gün geliştirmektedir. Otomotiv teknolojisi geliştikçe araç içerisinde insanların isteklerini yerine getiren birimlerin, elektronik kontrol ünitelerinin (ECU) sayısı da her

[1] *Yüksek Lisans Öğrencisi, İstanbul Aydın Üniversitesi Fen Bilimleri Enstitüsü, Elektrik Elektronik Mühendisliği Ana Bilim Dalı Küçükçekmece/İst. 05310322467, e-posta: serkanbaki@aydin.edu.tr, ORCID: 0000-0002-3753-0879*
[2] *Prof. Dr, İstanbul Aydın Üniversitesi Mühendislik Fakültesi, Elektrik-Elektronik Mühendisliği Bölümü, Küçükçekmece/İst. 05055839423, e-posta: nedimtutkun@aydin.edu.tr ORCID: 0000-0003-2750-5714*
DOI: 10.17932/IAU.ABMYOD.2006.005/abmyod_v16i61003

geçen gün artmaktadır. Araç içerisinde insanların isteklerine cevap veren elektronik kontrol ünitelerinin, haberleşmesinde gerçek zamanlı performansı ve verimli iletişiminden dolayı yaygın olarak denetleyici alan ağı (CAN) kullanılır. Ancak CAN haberleşmesinin ağ güvenliğinin nasıl sağlanacağı tartışmaları son zamanlarda oldukça artmıştır. Araştırmalara göre kontrolü basit ve doğası gereği güvenlik açığı olan bu haberleşme ağının kontrolü otomotiv korsanları tarafından kolayca ele geçirilebilir. Araç içerisinde CAN haberleşme ağına sızan korsanlar elektronik kontrol ünitelerini uzaktan kontrol ederek sadece araca değil insan sağlığına da etkilerinin olduğu yine araştırmalarda görülmüştür. Otomotiv teknolojisi gelişirken ortaya çıkan güvenlik açıklarına karşı sessiz kalmayan araştırmacılar alınması gereken önlemleri kendi makalelerinde işlemiştir. Bu araştırmanın amacı, araç içi haberleşme ağında korsan belirleme ünitesi (KBÜ) kurularak korsan varlığı belirlenip elektronik kontrol ünitelerinin birden fazla yoldan basit şifreli haberleşmesi sağlanarak saldırıları savuşturmaktır. Bu araştırma da kullanılan hibrit yöntem hem şifreli haberleşmeyi hem de saldırı belirleme ünitesini kapsamaktadır. Yöntemin bu hibrit yapısı denemelerin sonucunda CAN haberleşmesinde hem derinlemesine güvenliği sağlarken hem de kendisine ait doğal yapısından taviz vermemesini sağlamaktadır.

Anahtar Kelimeler: *Denetleyici alan ağı, şifreli haberleşme, korsan belirleme ünitesi, araçta ağ güvenliği, otomotiv saldırı tespiti*

Hybrid attack avoidance application for the controller area network in automotive communications

Abstract

As technology develops rapidly, people are usually expected to increase their life quality day by day, especially in the automotive sector. As the automotive technology develops, the number of units, electronic control units (ECU) that fulfil the wishes of the people in the vehicle is increasing as day pass. The controller area network (CAN) is widely used due to the real-time performance and efficient communication of electronic control units that respond to the requests of the people in their vehicle. However, discussions on how to secure the network of CAN communication have increased recently. According to research, the control of this communication network, which is simple to control and vulnerable in nature, can be easily taken over by automotive hackers. It has been seen in the researches that the hackers who infiltrated the CAN communication network in the vehicle have effects not only on the vehicle but also on human health by remotely controlling the electronic control units. The researchers, who did not remain silent against the security gaps that emerged as automotive technology developed, covered the precautions that should be taken in their articles. The aim of this research is to defend the attacks by establishing a hacker detection unit (KBU) in the in-vehicle communication network and determining the presence of hacker and providing simple encrypted communication of electronic control units in multiple ways. The hybrid method used in this research includes both encrypted communication and an attack detection unit. As a result of the experiments, this hybrid structure of the method mentioned in this study

provides both in-depth security in CAN communication and ensures that it does not compromise its canonical structure.

Keywords: *Controller area network, encrypted communication, hacker identification unit, in-vehicle network security, automotive intrusion detection*

Giriş

Günümüzde çoğu araç içi işlevsellik, daha iyi araç performansı, yolcu güvenliği ve gelişmiş eğlence tesisleri sağlamak için birbirine bağlı elektronik kontrol üniteleri (ECU) tarafından kontrol edilmektedir. Otomotiv teknoloji şirketleri her geçen gün yeni ürettikleri araçlarına yeni bir elektronik kontrol ünitesi eklemektedir. Modern arabalar içerisinde ortalama 70 ila 100 arası elektronik kontrol ünitesi içerebilir (Miller ve Valasek, 2015). ECU'lar, motor kontrolü, hava yastığı açılması ve kilitlenmeyi önleyici fren sistemi gibi güvenlik açısından kritik işlevler de dâhil olmak üzere otomobilin birçok önemli işlevlerinin çoğunu kontrol eder. Bu yüzden güvenli bir sürüşe sahip olmak için, ECU'lar güvenilir bir iletişim ağına sahip olmalıdırlar (Mundhenk, 2017).

Otomotiv teknolojisinde elektronik kontrol ünitelerinin haberleşmesinde yaygın olarak CAN haberleşmesi kullanılır (Miller ve Valasek, 2015). CAN ağı haberleşmede 2 tel kullanması kablolama gereksinimlerini ve araçların ağırlığını azaltır, bu da üreticiye daha düşük üretim maliyetleri ve tüketiciye daha düşük satın alma ve yakıt maliyeti sağlar. Elektriksel parazitlere karşı yüksek bağışıklık, kolay kablolama, kendi kendine teşhis yeteneği ve hataları onarma gibi tanınmış avantajları CAN veri yolunu otomobil endüstrisi için uygun hale getirir (URL 1). CAN elektriksel

gürültüye karşı dirençli olmasına ve güvenlik özelliklerine sahip olmasına rağmen, saldırılara karşı hala savunmasızdır. Bu haberleşme ağı otomotiv haberleşmesinde saldırılara karşı doğası gereği bazı güvenlik açıkları vardır. Örneğin veri iletiminde şifreleme ve kimlik doğrulama gibi ciddi güvenlik eksiklikleri vardır (Koscher ve ark., 2010).

Mevcut saldırılar

Modern otomobiller pasif hırsızlık önleme sistemi, lastik basıncı izleme sistemi, uzaktan anahtarsız giriş, bluetooth ve radyo gibi farklı tipte kablosuz arabirimlerle donatılmışlardır. Bu kablosuz arabirimler, güvenlik duvarı olan bir ağ geçidi ECU'su aracılığıyla CAN ağı ile iletişim kurabilirler. Bazı araştırmacılar güvenlik duvarlarını aşarlar ve CAN ağına erişirler. Valasek ve Miller bu güvenlik duvarını aşarak 12 otomobil markasının 21 otomobil modeline uzaktan 3 tip saldırı gerçekleştirdiler. Bu saldırılardan ilki kablosuz arabirimden sorumlu ECU'yu tehlikeye atmaktır. İkincisi güvenlik açısından kritik ECU ile iletişim kurmak için mesajlar enjekte etmektir. Üçüncüsü ise ECU'yu kötü niyetli davranacak şekilde değiştirmektir (Miller ve Valasek, 2014).

Diğer birçok çalışma, araç içi ağlardaki güvenlik açıklarını ve bu güvenlik açıklarına alınan farklı güvenlik önlemlerini göstermektedir. Bu saldırılar araç içi önemli ünitelere zarar vererek ya da üniteleri aldatarak kullanıcının hayatının kaybolmasına sebep verebilirler. Ayrıca araştırmacılar, otomobillerdeki artan siber-fiziksel sistemlerin güvenlik açıklarını daha da artıracağına inanıyorlar. Bu yüzden otomotiv teknolojisi geliştikçe CAN haberleşmesinde veri yolu güvenliği almak daha da önemli hale gelmiştir.

Bu nedenle, bu tür tehditlere karşı etkili önlemler geliştirmek acil bir konudur.

Mevcut önlemler

Otomotiv güvenliği yeni bir alan olduğu için bu alanda çözümlerin sayısı ve çeşitliliği de sınırlı kalmaktadır. Bununla birlikte CAN veri yolu güvenliğini iyileştirmek için önerilen bir dizi yaklaşım vardır. Bunlar şifreleme teknikleri, hedef şaşırtma teknikleri, saldırı tespit sistemleri (IDS) ve saldırı önleme sistemleri (IPS) olmak üzere 4 çeşittir (Nilsson ve Larson, 2009).

CAN protokolünde yayın niteliği nedeniyle bir şifreleme mekanizması bulunmadığından, bir saldırgan CAN trafiğini kolayca dinleyebilir ve iletişimi anlayabilir. Ayrıca herhangi bir düğümün ağa bağlanıp mesaj gönderebileceği anlamına gelen bir kimlik doğrulama özelliği olmadığından saldırgan bir düğüm CAN ağına veri çerçevesi gönderebilir ve diğer düğümler bunu kabul edip işleyebilir. Bu tür saldırıları önlemek ve gizlilik sağlamak için, araştırmacılar yazılım ve donanım düzeylerinde farklı şifreleme yöntemleri önermektedir. Birçok araştırmacı simetrik şifreleme yöntemlerini bir arada kullanarak yeni bir şifreleme yöntemi sunmuştur. Bazı şifreleme yöntemlerinin güvenlik hizmetlerini ve ağın çalışmasında önemli rol oynayan gereksinimleri nasıl etkilediğini bu makalede görebiliyoruz (Gmiden ve ark., 2019). Bu makalede şifreleme yöntemleri kullanılırken bazı değerlendirme ölçütleri kullanılmıştır. Bu ölçütler kimlik doğrulama, bütünlük, gizlilik, geriye dönük uyumluluk, tekrarlı saldırı direnci ve gerçek zamanlı başarıdır. Bu değerlendirme ölçütlerin sonuçları Tablo 1'de gösterilmiştir. Tablodaki işaretlerden (✓)

işareti gereksinimin karşılandığını (X) işareti gereksinimin karşılanmadığını ifade eder.

***Tablo 1**: Tanımlanmış gereksinimlere göre şifreleme yöntemlerinin katkıları (*Gmiden ve ark., 2019).

Şifreleme Yöntemi	Kimlik Doğrulama	Bütünlük	Gizlilik	Geriye Uyumluluk	Tekrarlı Saldırı Direnci	Gerçek Zamanlı Performans
LiBrA-CAN	✓	✓	X	X	X	X
WooAuth	✓	✓	✓	X	✓	✓
Vecure	✓	✓	X	✓	✓	X
CaCAN	✓	✓	X	X	✓	X
VatiCAN	✓	✓	X	✓	✓	X
VulCAN	✓	✓	X	✓	✓	X

Kimlik doğrulama: Kimlik doğrulama, veri mesajı ve ardından bir kimlik doğrulama mesajı gönderilerek gerçekleştirilir. Kimlik doğrulama mesajı şifreleme fonksiyonu ve gizli bir anahtar içeren mesaj doğrulama kodudur. Tablo 1'deki tüm şifreleme yöntemleri HMAC ve MAC kimlik doğrulama türü kullandığı için hepsi kimlik doğrulama ilkesini sağlar.

Bütünlük: Verilerin doğruluğu ve geçerliliği olarak tanımlanır. HMAC ve MAC sadece kimlik doğrulama değil aynı zamanda veri bütünlüğünü kontrol etmek içinde kullanılır. Tablo 1'deki tüm şifreleme yöntemleri

HMAC ve MAC kimlik doğrulama türü kullandığı için hepsi bütünlük ilkesini sağlar.

Gizlilik: Verilerin yalnızca yetkili kişilere sağlanması anlamına gelir. Tablo 1'de sadece WooAuth (Woo ve ark., 2014) şifreleme yöntemi veri iletiminde AES-128 şifreleme kullandığı için gizlilik ilkesini sağlar.

Geriye uyumluluk: CAN protokolünün doğal çerçeve yapısının bozulmamasıdır. Tablo 1'deki, Vecure (Wang ve Shawney, 2014), VatiCAN (Nurnberger ve Rossow, 2016) ve VulCAN (Bulck ve ark., 2017) şifreleme yöntemleri kimlik doğrulama verilerini kullanırken CAN veri çerçevelerini bozmadıkları için geriye uyumluluk ilkesini sağlarlar.

Tekrarlı saldırı direnci: CAN protokolünde geçerli bir kontrol veri çerçevesinin, saldırgan tarafından yeniden iletilmesine tekrarlı saldırı denir. Buna karşı konulan dirence de tekrarlı saldırı direnci denir. Tablo 1'de sadece LiBrA-CAN (Groza ve ark., 2012) şifreleme yöntemi hariç hepsi tekrarlı saldırı direnci ilkesini sağlar.

Gerçek zamanlı performans: CAN protokolünün veri iletişim hızı gerçek zamanlı olarak çalışır. Tablo 1'de sadece WooAuth (Woo ve ark., 2014) şifreleme yöntemi gecikmelere sebep olmayarak gerçek zamanlı performans ilkesini sağlar.

Genel olarak Tablo 1 incelendiğinde şifreleme yöntemlerinin CAN veri yolunun güvenliğini, kimlik doğrulama ve bütünlük ilkeleriyle artırıyor.

Ama aynı tabloda şifreleme yöntemlerinin çoğu, gizlilik ilkesinde bir şey yapamazken gerçek zamanlı uygulamalarda da gecikmelere sebebiyet veriyor. CAN protokolünde sınırlı bant genişliğini göz önüne alırsak şifreleme yöntemlerinin bir diğer kötü özelliği de kimlik doğrulama kullanarak CAN veri trafiğini iki katına çıkarmasıdır.

Denetleyici alan ağı (CAN)

CAN protokolü 1983 yılında otomotiv sektöründe kullanılmak üzere Robert Bosch tarafından geliştirilmeye başlanmıştır. Daha sonrasında Bosch firması tarafından 1986 yılında otomotiv topluluğuna duyurmuştur. Sonuç olarak CAN haberleşmesiyle birlikte otomobillerde merkezi ağ sistemine geçilmiştir. Intel tarafından 1987'de ilk CAN denetleyici yongası üretilmiştir. Başlangıçta yalnızca otomotiv sektöründe kullanılmaya başlanmıştır. Bu haberleşme ağı doğası gereği az yer kaplaması, güvenli olması ve yüksek hıza sahip olması gibi özelliklerinden dolayı daha sonrasında fabrika otomasyonunda, tıp elektroniğinde, tarım aletlerinde, asansör sistemlerinde, bina otomasyonlarında ve askeri uygulamalarda yaygın olarak kullanılmaya başlamıştır. CAN haberleşmesinin genel karakteristik özellikleri Tablo 2'de gösterilmiştir.

Tablo 2: *CAN haberleşmesi genel karakteristik* (URL 2)

İletişim Protokolü	İletişim Standardı	İletişim Tekniği	İletim Metodu	Haberleşme Hattı	Topoloji	Kontrol Tipi	Ortam Erişim Kontrol Metodu	İletim Ortamı	Maksimum Haberleşme Hızı
Seri İletişim	ISO 11898 ve ISO 11519	Yayın	Temel Bant	LAN	Bus Topolojisi	Dağıtık Kontrol	Multi Master	Çift Tel	1 Mbit/s

CAN protokolünde güvenlik açıklarının analizi

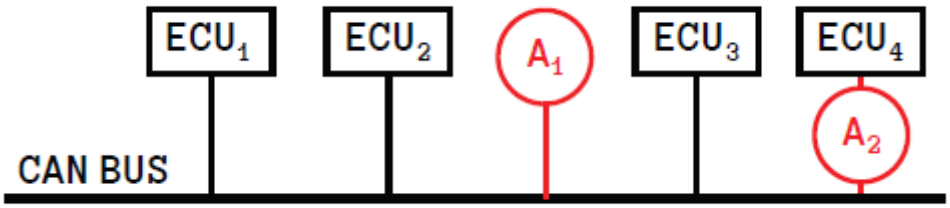
Bu bölümde CAN protokolü CIA (Gizlilik, Bütünlük ve Kullanılabilirlik) üçlüsüne göre analiz edilecektir. CIA üçlüsü, sistem güvenlik açığını değerlendirmek için basit bir güvenlik modelidir. CIA üçlüsü, herhangi bir güvenli sistemin sahip olması gereken üç temel ilkeyi analiz eder (Bozdal ve ark., 2018). CAN haberleşme ağı her ne kadar güvenli bir ağ olsa bile yine protokol içerisinde mevcut güvenlik açıkları vardır (Koscher ve ark., 2010). Bu güvenlik açıkları, korsanlar tarafından kasıtlı ve akıllı bir şekilde uygulandığında zarar ve zararlara yol açabilir.

Mesaj alış-veriş doğası: Gizlilik, verilerin yalnızca yetkili kişilere sağlanması anlamına gelir. Ancak CAN veri yolunda bir düğüm tarafından gönderilen CAN mesajı, veri yoluna bağlı tüm düğümler tarafından alınır. Böylece, Şekil 1'deki A1 veya A2 gibi bağlanan bir korsan ağ trafiğindeki veri çerçevelerini kolayca okuyabilir. Sonuç olarak CAN veri yolunda gizlilik söz konusu değildir.

Kimlik doğrulama yok: CAN veri çerçevelerinin kimlik doğrulayıcı alanları yoktur. Böylece, veri yoluna Şekil 1'deki A2 gibi bağlanan bir korsan herhangi bir düğümün kimliğini kullanarak sahte bir mesaj gönderebilir. Sonuç olarak CAN veri yolunda kimlik doğrulama söz konusu olmadığı için yetkisiz veri iletimi mevcuttur.

Mesaj öncelik doğası: Kullanılabilirlik, verilere veya ağa yetkili kullanıcı tarafından her zaman erişilebileceği anlamına gelir. Ancak CAN protokol gereği, veri yoluna aynı anda veri göndermeye çalışırsa, veri ID'si yüksek olan verinin iletileceğini söyler. Böylece, Şekil 1'deki A1 veya A2 gibi bağlanan bir korsan veri yolunu sürekli baskın bir mesaj göndererek DoS saldırılarına sebebiyet verebilir. Sonuç olarak CAN veri yolunda kullanılabilirlik söz konusu değildir.

Döngüsel artıklık kontrolü (CRC): Bütünlük, verilerin doğruluğu ve geçerliliği olarak tanımlanır. Veri iletim sırasında değiştirilmemelidir. CAN protokolünde, bir mesajın değiştirilip değiştirilmediğini doğrulamak için CRC kullanır. Ancak, bir CRC saldırganın veri çerçevesini değiştirmesini engelleyemez. Sonuç olarak CAN veri yolunda bütünlük de söz konusu değildir.



Şekil 1: *CAN haberleşmesinde korsan bağlantı şekilleri (Boudguiga ve ark., 2016).*

CAN protokolünde güvenlik açıklarından dolayı oluşan saldırılar

Yukarıda yapılan güvenlik analizine ve çıkan güvenlik açıkları göz önüne alındığında CAN ağında saldırılar üç gruba ayrılır:

Gizlice dinleme: CAN ağını gizlice dinleme birçok saldırının başlangıç noktasıdır. CAN ağında veri mesajları arasında şifreleme eksikliği, herhangi bir düğümün veri yolu trafiğini anlamasına izin verir, böylece bir korsan CAN verilerini okuyabilir ve bilgileri toplayabilir. Gizlice dinleme pasif saldırı olarak sınıflandırılabilir, bu nedenle iletişimi bozmaz. Ancak, aktif saldırılara yol açabilir. Örneğin, Palanca ve arkadaşları bu makalede (Zanero ve ark., 2010) CAN verilerini okudular ve saldırmayı planladıkları park sensörü düğümünün kimliğini ve verilerini belirlediler. Daha sonrasında bu düğüme bir DoS saldırısı uyguladılar.

Veri ekleme: Yetkisiz CAN düğümünün mevcut veri yoluna veri çerçevesi eklenmesi olarak tanımlanabilir. CAN protokolünde bir kimlik doğrulama mekanizması olmadığından, saldırgan bir düğüm ağa bağlanabilir ve istediği düğüme bir veri gönderebilir. Koscher ve arkadaşları bu

araştırmada aracın OBD-II portundan CAN ağına sızdılar (Koscher ve ark., 2010). Daha sonrasında aracın hayati üniteleri olan gösterge panelini, fren kontrol ünitesini ve motor kontrol ünitesini çözümlediler. Yakıt seviyesini ve hız göstergesi değerlerini değiştirdiler ve gösterge panelinde yanlış veri gösterdiler. Ayrıca motoru devre dışı bırakabildiler ve devir / dakika gibi motor parametrelerini değiştirebildiler.

Hizmet reddi (DoS): DoS saldırıları belirli bir düğümü, düğümleri veya tüm ağı hizmet vermesini engelleyen saldırılardır. Palanca ve arkadaşları bu araştırmada ağa gizli bir düğüm ekleyerek seçici DoS saldırısı uyguladılar (Zanero ve ark., 2010). Saldırgan düğüm, ağın tanımlı verici düğümünün veri yoluna gönderdiği bir veri çerçevesinin bitlerinin üzerine yazar ve hata çerçevesi oluşturur. CAN protokolünün hata sınırlaması nedeniyle, belirli sayıda hata oluştuktan sonra verici düğümü veri yoluna kapalı durumuna geçer ve artık kullanılamaz. Saldırı yöntemi veri yoluna bağlı herhangi bir düğümü devre dışı bırakabilir.

Hibrit saldırı savuşturma metodu

Güvenlik mekanizması, bir saldırının gerçekleşmesini önlemek için ya da saldırının etkisini en aza indirmek için tasarlanmış önlemlerdir. Otomotiv sistemlerinin karmaşıklığı nedeniyle, tek bir mekanizmanın uygulanması bütün saldırıları engelleyemez. Bu nedenle, riskleri en aza indirmek için son güvenlik mekanizmalarının kullanılmasına dayanan 'derinlemesine savunma' stratejisi benimsenmelidir. Derinlemesine savunma saldırıları ele almak için dört yaklaşım sunar (Nilsson ve Larson, 2009) :

Önlem: Bir saldırının gerçekleşme olasılığını engellemek için derinlemesine alınmış önlemler zinciridir. Simetrik ve asimetrik şifreleme türleri buna örnektir.

Hedef saptırma: Bir saldırganın bir yemle tepki verirken saldırıyı başardığına inanmasına yol açan tekniktir.

Tespit: Bir saldırganın izinsiz giriş sonrasında veri yoluna izinsiz veri göndermesi ile sistemin normal aktivitesi arasında ayrım yapmasıdır.

Koruma: Bir saldırganın izinsiz giriş durumu algılanıp hemen otomatik olarak tepki vererek saldırının önlenmesi tekniğidir.

CAN ağında derinlemesine güvenlik sağlamak için genellikle araştırmacılar tarafından kullanılan 2 popüler konu, saldırı tespit sistemleri ve şifreleme yöntemleridir. Araştırmacılar CAN ağında bu 2 güvenlik yöntemini kullanılırken hem mevcut güvenlik açıklarını (kimlik doğrulama ve gizlilik eksikliği) çözüm getirirken hem de ağın gerçek zamanlı performansına dikkat ederler.

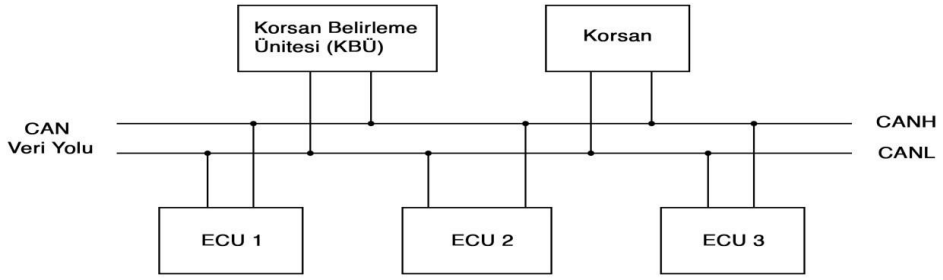
Saldırı tespit sistemleri (IDS) CAN ağında elektronik kontrol üniteleri üzerindeki anormal veya şüpheli etkinlikleri tanımlamak için tasarlanmış sistemlerdir. CAN ağı için birçok tanımlanmış saldırı davranışları vardır. Kullanılan tespit yöntemine bağlı olarak temelde iki tip IDS tekniği vardır (Gmiden ve ark., 2019). Bunlar senaryo yaklaşımı kullanan ve davranışsal yaklaşımı kullanan sistemlerdir. Senaryo yaklaşımında, IDS bir saldırı

senaryosu için veri tabanı kullanır. Şüpheli davranışları tespit ettiği anda bir uyarı verir. Senaryo yaklaşımı saldırıları çok hassas bir şekilde yönetmeyi mümkün kılar. Ancak senaryo veri tabanı güncellenmezse, IDS sistemi bilinmeyen saldırıları algılayamayabilir. Davranışçı yaklaşımında ise izlenecek sistemin beklenen zamanda veri alış-verişi yapmasına dayanır. Senaryo yaklaşımının aksine, bu yaklaşım saldırıları bilinmese bile tespit edebilir.

Şifreleme yöntemleri, verilerin gizli bir forma dönüştürülmesini içeren yöntemlerdir. Şifreleme yöntemleri, otomotiv sistemleri için gizlilik, bütünlük ve kimlik doğrulama için olası bir çözümdür. Şifreleme yöntemlerinde, simetrik ve asimetrik olmak üzere 2 tip anahtar kullanılır. Simetrik anahtarlar başlangıçta tüm cihazlara dağıtılırlar ve keşfedilmeleri daha kolaydır. Asimetrik anahtarlar ise daha karmaşık bir yapıya sahip olduklarından daha güvenlidir ama eklendiği gömülü sistemin işlem gücü kapasitesini etkiler, bu da maliyetin artmasına neden olabilir (Diffie ve Hellmann, 2019).

Derinlemesine savunma sistemi analiz edildikten sonra araç içi denetleyici alan ağına (CAN) bağlı olan elektronik kontrol ünitelerini korsan saldırılara karşı korumak için hem saldırı tespit sistemi hem de elektronik kontrol üniteleri arasında ilkel şifreleme yöntemleri ile mesajlaşan hibrit bir uygulama geliştirilir. Bu uygulamada Şekil 2'deki gibi araç içi CAN ağını temsil eden bir veri yolu kurulur. Korsan belirleme ünitesi (KBÜ) hem kendine has yöntemlerle korsan varlığını belirlerken hem de korsan ünitesinin veri yolundaki elektronik kontrol ünitelerinin mesajlarını

çözmesin diye şifreli mesaj değiştirme emirleri verir. Kurulan bu sistem kendine has basit şifreleme yöntemleri ve saldırı tespit sistemi ile birlikte hibrit olarak çalışarak CAN veri yolunun güvenliğini sağlamış olur.



Şekil 2: *CAN veri yolunda saldırı savuşturma uygulaması*

Bulgular

Otomotiv haberleşme ağında incelenen mevcut saldırı savuşturma uygulamaları ile bu makalede anlatılan hibrit saldırı savuşturma uygulaması Tablo 3'de karşılaştırıldı.

Tablo 3: *Mevcut şifreleme yöntemleri ile geliştirilmiş uygulamaların hibrit saldırı savuşturma uygulaması ile karşılaştırılması*

Şifreleme Yöntemi	**Kimlik Doğrulama**	**Bütünlük**	**Gizlilik**	**Geriye Uyumluluk**	**Tekrarlı Saldırı Dirençi**	**Gerçek Zamanlı Performans**	**Saldırı Tespit Sistemi**
LiBrA-CAN	✓	✓	X	X	X	X	X
WooAuth	✓	✓	✓	X	✓	✓	X
Vecure	✓	✓	X	✓	✓	X	X
CaCAN	✓	✓	X	X	✓	X	X
VatiCAN	✓	✓	X	✓	✓	X	X
VulCAN	✓	✓	X	✓	✓	X	✓
Hibrit Yöntem	X	✓	X	✓	✓	✓	✓

Kimlik doğrulama: Veri mesajından sonra kimlik doğrulama için gönderilen mesajlar CAN ağında güvenliği artırıyor ama öte yandan veri trafiğini artırarak CAN haberleşme protokolünün gerçek zamanlı performansını etkiliyor. Otomotiv teknolojisinde CAN haberleşme ağı gerçek zamanlı performansı ve verimli iletişiminden dolayı yaygın olarak kullanıldığı için hibrit saldırı savuşturma yöntemimiz CAN haberleşme ağının gerçek zamanlı performansını etkilememek için kimlik doğrulama mesajları göndermemeyi tercih ederek kimlik doğrulama ilkesini sağlamaz.

Bütünlük: Hibrit saldırı savuşturma uygulamamız içerisinde kullanılan basit simetrik şifreleme yöntemi kendi içerinde bir CRC'ye sahip olup verilerin doğruluğu ve geçerliliği ilkesi olan bütünlük ilkesini sağlar.

Gizlilik: Hibrit saldırı savuşturma uygulamamız CAN ağında mevcut çerçeve yapısını bozmayıp her ağa kolay uyumluluk sağlamak için verileri yetkili kişilere değil CAN ağına göndermeyi tercih ederek gizlilik ilkesini sağlamaz.

Geriye uyumluluk: Geriye uyumluluk mevcut CAN çerçeve yapısını bozmayarak mevcut sisteme daha hızlı adapte olmayı sağlar. Hibrit saldırı savuşturma uygulamamız gizlilik ilkesini sağlamayarak geriye uyumluluk ilkesini sağlar.

Tekrarlı saldırı direnci: Hibrit saldırı savuşturma uygulamamızdaki ilkel simetrik şifreleme yöntemimiz belirli aralıklar ile sürekli şifrelenen anahtarı değiştirdiği için CAN ağında aynı işlem için farklı mesajlar bulunacaktır. Bu sayede saldırgan son gönderilen mesaj ile kontrolü sağlayamayacaktır.

Gerçek zamanlı performans: CAN ağında bir görev için bir mesajdan fazlası gönderilirse CAN ağında veri trafiği artar ve CAN ağının gerçek zamanlı performansı ortadan kaybolur. Tablo 3'te bu duruma aykırı görünen WooAuth (Woo ve ark., 2014) şifreleme yöntemi mevcut CAN çerçeve yapısını bozduğu için gerçek zamanlı performansı sağlarken geriye uyumluluğu sağlamaz. Hibrit saldırı savuşturma uygulamamız ise

hem geriye uyumluluğu hem de gerçek zamanlı performans ilkelerini sağlayarak CAN haberleşme protokolünün otomotiv teknolojisinde kullanılma sebeplerini sağlamış olur.

Saldırı tespit sistemi: Hibrit saldırı savuşturma uygulamamızın bir diğer yöntemi olan saldırı tespit sistemi Tablo 3'te gösterildiği üzere diğer uygulamalarda bulunmamaktadır. Saldırı tespit sistemi korsan varlığını algılayıp anahtar değişikliği, CAN ağına DoS saldırısı düzenleme ve raporlama aksiyonlarını yaparak diğer uygulamalardan bir adım önde olduğunu göstermektedir.

Sonuçlar

Bu makalede otomotiv içerisindeki ECU'ların birbirleri ile haberleşmesi için kullandığı CAN haberleşme protokolünü ve CAN haberleşmesindeki mevcut güvenlik açıklarını ele aldık. Ayrıca literatürde CAN haberleşme protokolü üzerinden kablolu ya da kablosuz şekilde otomobil içerisindeki ECU'lara sızma örneklerini özetledik. Araçlardaki ECU'larda kablosuz haberleşme protokollerinin kullanımı artıkça kablosuz saldırıların da artacağını saptadık. CAN haberleşme protokolünde doğası gereği oluşan güvenlik açıklarına karşı alınması gereken tüm önlemleri derinlemesine savunma başlığı altında inceledik. Derinlemesine savunma yöntemlerinden yola çıkarak popüler olarak kullanılan iki popüler konu olan saldırı tespit sistemleri (IDS) ve şifreleme yöntemlerini analiz ettik.

CAN veri yolunda kimlik doğrulama için sadece şifreleme yöntemleri kullanılırsa bant genişliği ve gerçek zamanlı performans gibi CAN ağının çalışmasında önemli rol oynayan özellikler kötü etkileneceğini gösterdik. Ayrıca CAN veri yolunda gizlilik ilkesini sağlama için geriye uyumluluk ilkesini bozmanın mevcut CAN ağlarında adapte sorunu ortaya çıkaracağını saptadık. Bu nedenle, CAN ağında güvenlik sağlanırken uygulanabilirlikten uzaklaşmayan çözümün, ilkel şifreleme yöntemi ve IDS den oluşan hibrit bir sistemle elde edilebileceğini saptadık.

Kaynaklar

[1] Boudguiga, A. Klaudel, W. Boulanger, A. and Chiron, P. (2016). A Simple Intrusion Detection Method for Controller Area Network, *2016 IEEE International Conference on Communications (ICC)*

[2] Bozdal, M. Samie, M. and Jennions, J. (2018). A Survey on CAN Bus Protocol: Attacks, Challenges, and Potential Solutions, *2018 International Conference on Computing, Electronics & Communications Engineering*

[3] Bulck, J.V. Muhlberg, J. T. and Piessens, F. (2017).VulCAN: Efficient Component Authentication and Software Isolation for Automotive Control Networks, *ACSAC 2017*

[4] Diffie, W. and Hellmann, M. E. (1979). Privacy and Authentication: A Introduction to Cryptography, *Proceedings of the IEEE*

[5] Gmiden, M. Gmiden, M. H. and Trabelsi, H. (2019). Cryptographic and Intrusion Detection System for automotive CAN bus Survey and contributions, *2019 16th International Multi-Conference on Systems, Signals & Devices (SSD).*

[6] Groza, B. Murvay, S. Herrewege, A. V. and Varbeuwhede, I. (2012). LiBrA-CAN: A Lightweight Broadcast Authentication Protocol for Controller Area Networks, *International Conference on Cryptology and Network Security*.

[7] Koscher, K. Czeskıs, A. Roesner, F. Patel, S. Kohno, T. Checkoway, S. Mccoy, D. Kantor, B. Anderson, D. Shacham, H. and Savage, S. (2010). Experimental Security Analysis of a Modern Automobile, *IEEE Symposium on Security and Privacy*

[8] Miller, C. and Valasek, C. (2014). A Survey of Remote Automotive Attack Surfaces, *BlackHat*

[9] Miller, C. and Valasek, C. (2015). Remote Exploitation of an Unaltered Passenger Vehicle, *BlackHat.*

[10] Mundhenk, P. (2017). Security for Automotive Electrical / Electronic (E/E) Architectures, *Cuvillier Verlag,* Göttingen

[11] Nilsson, D. K. and Larson, U. E. (2009). A Defense-in-Depth Approach to Securing the Wireless Vehicle Infrastructure, *Journal of Networks*

[12] Nurnberger, S. and Rossow, C. (2016). vatiCAN -Vetted, Authenticated CAN Bus, *International Conference on Cryptographic Hardware and Embedded Systems.*

[13] R. Kurachi, Y. Matsubara, H. Takada, N. Adachi, Y. Miyashita and S. Horihata, (2014). CaCAN - Centralized authentication system in CAN (controller area network), *14th Int. Conf. on Embedded Security in Cars ESCAR.*

[14] Wang, Q. and Sawhney, S. (2014). VeCure: A Practical Security Framework to Protect the CAN Bus of Vehicles, *2014 International Conference on the Internet of Things (IOT).*

[15] Woo, S. Jo, H. J. and Lee, D. H. (2014). A Practical Wireless Attack on the Connected Car and Security Protocol for In-Vehicle CAN, *IEEE Transactions On Intelligent Transportation Systems.*

[16] Zanero, S. Palanca, A. Evenchick, E. and Maggi, F. (2017). A Stealth, Selective, Link Layer Denial-of-Service Attack Against Automotive Networks*, in International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment.*

İnternet Kaynakları

[1] URL 1-http://esd.cs.ucr.edu/webres/can20.pdf/, (Erişim tarihi: 04.01.2021).

[2] URL 2-https://en.wikipedia.org/wiki/CAN_bus/, (Erişim tarihi: 04.01.2021).