**Literatür Taraması**

**Otonom Araçlarda Siber Güvenlik: Controller Area Network Bus Protokolü Üzerinden Saldırı Analizi**

**1. Giriş**

Günümüzde otomotiv endüstrisi, araçların fonksiyonlarını ve sürüş konforunu artırmak amacıyla elektronik kontrol üniteleri (ECU) ve sensörler gibi bileşenleri yoğun bir şekilde kullanmaktadır. Bu bileşenler, araç içi haberleşmeyi sağlamak için Controller Area Network (CAN) protokolünü kullanır. Controller Area Network, düşük maliyetli, dayanıklı ve gerçek zamanlı veri iletimi özellikleri ile öne çıkarken, tasarımında güvenlik önlemlerinin bulunmaması nedeniyle siber saldırılara karşı oldukça savunmasızdır. Özellikle otonom araçlarda, artan ECU sayısı, dış bağlantıların (ör. Internet of Things, OTA güncellemeleri, V2X iletişimi) varlığı ve yazılım karmaşıklığının artması, siber güvenlik risklerini katlanarak yükseltmektedir.

Bu literatür taraması, Controller Area Network bus protokolü ve onun üzerinden gerçekleştirilen saldırılar ile ilgili mevcut akademik çalışmaları inceleyerek, bu alanda kullanılan güvenlik yöntemlerini ve önerilen çözümleri derinlemesine analiz etmektedir. Çalışmada özellikle üç temel makale – Controller Area Network protokolünün zafiyetleri, Controller Area Network saldırılarını önlemek için Secure Boot temelli yaklaşımlar ve Controller Area Network bus üzerinde gerçekleştirilen saldırı deneyleri ile IDS (Intrusion Detection System) uygulamaları ele alınmış ve sentezlenmiştir.

**2. Controller Area Network Bus Protokolü: Temel Yapı ve Güvenlik Zafiyetleri**

**2.1. Controller Area Network Bus’ın Temel Özellikleri**

CAN (Controller Area Network) protokolü, 1980’lerde Bosch tarafından geliştirilmiş ve otomotiv uygulamaları için standart hâline gelmiş akıllı bağlantılı araçlarda elektronik ve elektronik sistemler arasındaki iletişim için yaygın olarak kullanılan bir veri yolu protokolüdür. Temel özellikleri şunlardır:

* **Yayın Tabanlı Haberleşme:**  
  Tüm ECU’lar aynı veri hattını (twisted pair) paylaşır ve gönderilen mesajlar tüm nodlara ulaşır. Bu durum, iletişimde esneklik sağlar ancak aynı zamanda güvenlik zafiyetlerine de yol açar.
* **Diferansiyel İletim:**  
  Controller Area Network, elektromanyetik parazitlere karşı dayanıklı olması için diferansiyel sinyal iletimi kullanır. CAN\_H (yüksek) ve CAN\_L (düşük) hatları arasındaki sinyal farkı, verinin alınmasını sağlar.
* **Gerçek Zamanlı İletişim:**  
  Maksimum 1 Mbps hızında veri iletimi sağlayan Controller Area Network, özellikle motor kontrolü, frenleme ve güvenlik sistemlerinde zaman duyarlılığını karşılar.
* **Hata Tespiti Mekanizmaları:**  
  Protokol, CRC, ACK, bit stuffing gibi hata kontrol yöntemleriyle veri bütünlüğünü sağlamaya çalışır.

**2.2. Güvenlik Zafiyetleri**

Controller Area Network protokolü, başlangıçta sadece veri iletimi ve hata kontrolü odaklı geliştirildiği için güvenlik mekanizmaları (şifreleme, kimlik doğrulama, bütünlük kontrolü) entegre edilmemiştir. Bu durum, aşağıdaki zafiyetlere neden olmaktadır:

* **Şifreleme Eksikliği-Lack of Encryption:**  
  Tüm Controller Area Network mesajları açık metin olarak iletilir. Bu nedenle, ağ trafiğini dinleyen bir saldırgan, gönderilen verileri doğrudan okuyabilir.
* **Kimlik Doğrulama Yokluğu-No Authentication Mechanism:**  
  ECU’lar arasında mesaj göndericisinin doğrulanması yapılmadığından, sahte ECU’lar veya kötü niyetli yazılım tarafından gönderilen mesajlar tespit edilemez.
* **Ağ Segmentasyonu Eksikliği-Network Segmentation Absence:**  
  Tek bir ECU’da gerçekleştirilen saldırı, tüm ağa sıçrayabilir; çünkü tüm ECU’lar aynı fiziksel veri yolunu paylaşır.
* **Öncelik Tabanlı Çatışma (Arbitration) Mekanizması- Priority-Based Arbitration Mechanism:**  
  Yüksek öncelikli mesajların öncelikli olarak iletilmesi, saldırganın yüksek öncelikli sahte mesajlar göndererek diğer mesajların iletilmesini engellemesine olanak tanır (DoS saldırısı).

Bu zafiyetler, otonom araçlarda kritik fonksiyonların (ör. fren, direksiyon kontrolü) kötü niyetli kişilerce ele geçirilmesi gibi ciddi güvenlik risklerine yol açmaktadır.

**3. Mevcut Saldırı Senaryoları ve Deneysel Bulgular**

**3.1. Controller Area Network Bus Üzerinde Gerçekleşen Saldırılar**

Literatürde bildirilen saldırı senaryoları genel olarak iki ana kategoriye ayrılmaktadır:

1. **Fiziksel Erişim Temelli Saldırılar:**
   * **OBD-II Portu Üzerinden Saldırı-OBD-II Port Exploitation:**  
     Araçların OBD-II (On-Board Diagnostics) portu üzerinden doğrudan Controller Area Network hattına bağlanarak mesajlar okunabilir ve manipüle edilebilir.
   * **Kötü Amaçlı ECU Eklenmesi-Malicious ECU Injection:**  
     Fiziksel olarak aracın veri yoluna bağlanarak sahte ECU’lar eklenebilir ve bu ECU’lar üzerinden kötü amaçlı mesajlar gönderilebilir.( Araçtaki farklı kontrol ünitesi (örneğin motor kontrol, fren sistemi, hava yastığı sistemi vb.) her biri bir ECU olarak görev yapar.)
2. **Uzaktan Yapılan Saldırılar:**
   * **Kablosuz Bağlantılar (Wi-Fi, Bluetooth, 4G/5G) Üzerinden Saldırı:**  
     Araçların dışa açık bağlantı noktaları kullanılarak, uzaktan kötü amaçlı kod enjeksiyonu yapılabilir.
   * **Fuzzing ve Sniffing:**  
     Rastgele veya bozuk verilerin gönderilmesiyle ECU’ların beklenmeyen davranışlar sergilemesi sağlanabilir. Ayrıca, ağ trafiği dinlenerek kritik bilgilerin ele geçirilmesi mümkün olabilir.

**3.2. Controller Area Network veri yolu protokolüne yönelik yaygın saldırılar**

* **Mesaj Enjeksiyonu(Message Injection):** Saldırganlar Controller Area Network veri yoluna yanlış mesajlar enjekte edebilir ve ECU'lara yetkisiz komutlar göndererek araç davranışını değiştirebilir.
* **Spoofing:** Bu, bir saldırganın veri yolunda daha yüksek öncelik kazanmak için sahte bir kimlikle mesajlar göndermesini ve meşru iletişimleri bozmasını içerir.
* **Hizmet Reddi (Denial of Service-DoS):** Saldırganlar ağı yüksek öncelikli mesajlarla doldurarak meşru mesajların iletilmesini engelleyebilir ve bu da sistem arızalarına yol açabilir.
* **Veri Manipülasyonu(Data Manipulation):** Fiziksel katmanda saldırganlar, iletim sırasında mesaj içeriğini değiştirerek bit-flip'ler oluşturarak verileri manipüle edebilir.
* **Gizlice Dinleme ve Tekrar Oynatma(Eavesdropping and Replay):** Saldırganlar CAN veri yolundaki mesajları yakalayabilir ve yetkisiz eylemlere neden olmak için bunları yeniden oynatabilir.

**3.3. Deneysel Bulgular**

Birçok çalışma, gerçek araçlar üzerinde yapılan deneylerle bu saldırı senaryolarını doğrulamaktadır. Örneğin:

* **Jeep Cherokee Hack Olayı (2015):**  
  Araç, uzaktan erişim sağlayarak hacklenmiş ve kritik sistemleri (fren, direksiyon) kontrol altına alınmıştır.
* **Sahte Mesaj Injection Deneyleri:**  
  Deneysel çalışmalar, belirli mesaj ID’lerinin (örneğin, motor devri bilgisi için 0x186) sahte veri ile değiştirilmesinin gösterge panelinde hatalı bilgi üretmesine yol açtığını göstermiştir.
* **Frekans Analizi Tabanlı IDS Deneyleri:**  
  Gerçek ECU’ların belirli sabit frekansta gönderdiği mesajlarla, saldırganın yüksek frekansta sahte mesaj enjekte etmesi durumunda, aradaki zaman farkı tespit edilerek IDS sistemleri başarılı bir şekilde saldırıyı algılayabilmektedir.

**4. Mevcut Güvenlik Çözümleri ve Yaklaşımlar**

**4.1. Kriptografik Yöntemler**

Literatürde, Controller Area Network Bus üzerinde şifreleme ve kimlik doğrulama yöntemlerinin uygulanması önerilmektedir. Bu yaklaşımlar arasında:

* **AES-128 Tabanlı Şifreleme:**  
  Mesajların şifrelenmesi ile dinleme saldırılarının etkisi azaltılabilir. Ancak, tüm ECU’ların bu şifreleme yöntemini desteklemesi gerekmekte ve ek işlem yükü getirmektedir.
* **MAC (Message Authentication Code) ve Dijital İmzalar:**  
  Gönderilen mesajların bütünlüğü ve kaynağı, MAC algoritmaları ve dijital imza yöntemleri ile doğrulanabilir. Bu yöntemler, özellikle ECU spoofing saldırılarına karşı etkilidir.

**4.2. Saldırı Tespit Sistemleri (IDS-Intrusion Detection Systems)**

IDS sistemleri, Controller Area Network mesajlarının normal davranışlarından sapmaları tespit ederek anormal aktiviteleri uyarı olarak raporlar. Yaklaşımlar şu şekilde sınıflandırılabilir:

* **Imza Tabanlı IDS:**  
  Bilinen saldırı desenlerine göre anormallik tespit eder. Yeni veya bilinmeyen saldırıları yakalamada sınırlı kalabilir.
* **Anomali Tabanlı IDS:**  
  Makine öğrenmesi ve derin öğrenme yöntemleri kullanılarak, CAN mesajlarının zamanlama, frekans, veri payload gibi özelliklerine dayalı olarak anormal durumlar belirlenir. Örneğin, belirli bir mesajın gönderilme sıklığındaki artış veya zamanlamadaki sapmalar saldırı belirtisi olarak algılanabilir.

**4.3. ECU Seviyesinde Güvenlik: Secure Boot Yaklaşımı**

Özellikle otonom araçlarda, saldırıların temel nedeni olarak kötü amaçlı yazılımın ECU’lara sızması öne çıkmaktadır. Bu nedenle, ECU’nun başlatılması sırasında yazılımın bütünlüğünün doğrulanması (Secure Boot) önemli bir çözüm olarak sunulmaktadır:

* **Secure Boot Süreci:**  
  ECU başlatılırken, depolanmış referans değerle karşılaştırılması için yazılımın kriptografik hash değeri hesaplanır. Eğer yazılımın hash değeri değiştirilmişse, sistem çalışmaya izin vermez.

Secure boot için Güvenlik Algoritmalarının Karşılaştırılması

|  |  |  |
| --- | --- | --- |
| Algorithm | Security | Performance |
| CMAC | Medium | High |
| ECDSA | High | Low |
| HMAC-SHA256 | Medium-High | Medium |
| RSA-PSS | Very High | Low |
| ECDSA-CMAC (Proposed Solution) | Very High | Optimized Performance |

* **Veri Bütünlüğü Algoritmaları:**  
  SHA-256, HMAC, CMAC, ECDSA ve RSASSA-PSS gibi algoritmalar test edilmiş ve performans/güvenlik dengesi değerlendirilmiştir. Özellikle, ECDSA-CMAC gibi hibrit yaklaşımlar, hem yüksek güvenlik hem de hızlı işlem süreleri sunarak öne çıkmaktadır.

**5. Controller Area Network veri yolu güvenliğini artırmak için çeşitli gelişmiş algılama sistemleri önerilmiştir.**

Bunlar şunları içerir:

* **Derin Öğrenme Yaklaşımları(Deep Learning Approaches):** Konvolüsyonel sinir ağları (CNN) ve hibrit CNN-LSTM modelleri kullanan yüksek performanslı bir sistem, saldırı mesajlarını yüksek doğrulukla (%97,30) tespit etmek ve sınıflandırmak için geliştirilmiştir.
* **Çapraz Zincir İzinsiz Giriş Tespiti(Cross-Chain Intrusion Detection):** CCID-CAN modeli, ilk tespit için kural tabanlı bir geçerli bit endeksi (VBIN) kullanmakta, ardından gözden kaçan saldırıları belirlemek için Kalman filtresi ve Naïve Bayes modellerini kullanmaktadır. Bu model aynı zamanda bağlı araçlar arasında saldırı günlüğü alışverişini kolaylaştırarak tespit performansını optimize eder.
* **İzolasyon Ormanı Yöntemi(Isolation Forest Method):** Geliştirilmiş bir izolasyon ormanı yöntemi (MS-iForest), anomali puanlaması için veri yığınını kullanır, veri kurcalama saldırılarını etkili bir şekilde tespit eder ve diğer anomali tespit şemalarından daha iyi performans gösterir.
* **Spesifikasyon Tabanlı Tespit(Specification Based Detection):** SAIDuCANT sistemi, anomali tabanlı saldırı tespiti için gerçek zamanlı Controller Area Network veri yolu model parametrelerini kullanır ve veri enjeksiyon saldırılarını tespit etmede düşük yanlış pozitif oranlara ulaşır.

**6. Geleceğe Yönelik Çalışmalar ve Öneriler**

Otonom araçların güvenliğinin sağlanması, sadece mevcut yöntemlerin iyileştirilmesiyle sınırlı kalmamakta, aynı zamanda yeni teknolojilerin entegrasyonu ile de desteklenmelidir. Gelecekte üzerinde çalışılması gereken başlıca konular şunlardır:

* **Post-Kuantum Kriptografi:**  
  Kuantum bilgisayarların klasik kriptografik yöntemleri tehdit etmesi göz önüne alınarak, post-kuantum algoritmaların Controller Area Network Bus güvenliğinde uygulanabilirliği araştırılmalıdır.
* **Hibrit Güvenlik Sistemleri:**  
  Secure Boot, IDS ve şifreleme gibi yöntemlerin birlikte kullanıldığı çok katmanlı güvenlik mimarileri geliştirilmelidir. Böylece, tek bir yöntemin başarısız olması durumunda diğer katmanlar sistemi koruma altına alabilir.
* **Gerçek Zamanlı Veri Analizi:**  
  Makine öğrenmesi ve derin öğrenme tabanlı IDS sistemlerinin, gerçek zamanlı veri analizi yapabilmesi için optimize edilmesi gerekmektedir. Bu sistemlerin, anormal durumları düşük gecikme ile tespit etmesi, özellikle kritik uygulamalarda büyük önem taşır.
* **Fiziksel Erişim Kontrolleri:**  
  OBD-II portu gibi araç içi fiziksel erişim noktalarının korunması için donanımsal güvenlik önlemleri (kilitli portlar, erişim kontrol modülleri) geliştirilmelidir.
* **İnteraktif Simülasyon ve Deneysel Çalışmalar:**  
  Gerçek araçlar veya simülasyon ortamlarında gerçekleştirilecek deneysel çalışmalar, önerilen güvenlik sistemlerinin etkinliğini ölçmek ve optimize etmek açısından önemli veriler sağlayacaktır.

**6. Sonuç**

Literatür taraması sonucunda, Controller Area Network Bus protokolünün orijinal tasarımında güvenlik önlemlerinin bulunmaması, modern araçlardaki artan ECU sayısı ve bağlantı noktaları nedeniyle ciddi güvenlik açıklarına yol açtığı belirlenmiştir. Mevcut çalışmalar, hem saldırı senaryolarını detaylandırmış hem de çeşitli güvenlik çözümlerini (kriptografik yöntemler, IDS sistemleri, Secure Boot) ortaya koymuştur. Tez çalışmanız kapsamında, bu yaklaşımların birleştirildiği hibrit güvenlik mimarileri üzerinde yoğunlaşarak, otonom araçların siber güvenliğini artırmaya yönelik yenilikçi çözümler geliştirme potansiyeli bulunmaktadır.

Özetle, bu literatür taraması;

* **Controller Area Network Bus’ın yapısal güvenlik eksikliklerini,**
* **Gerçek saldırı senaryolarını ve deneysel bulguları,**
* **Mevcut güvenlik yaklaşımlarının avantaj ve dezavantajlarını,**
* **Ve geleceğe yönelik araştırma alanlarını** detaylı olarak ele almaktadır.

**Kaynakça (Örnek)**

1. Bobbala, M. R., & Kavitha, R. “Analyzing the CAN Protocol Vulnerabilities, Protective Measures and Improvements.”
2. Salah Adly, Ahmed Moro, Sherif Hammad,Shady A. Maged “Prevention of Controller Area Network (CAN) Attacks on Electric Autonomous Vehicles.”
3. Karrouchi, M., et al. “Analysis of current attacks on the CAN bus and development of a new solution to detect these types of malicious threats.”
4. Miller, C., & Valasek, C. “A survey of remote automotive attack surfaces.”
5. Koscher, K., et al. “Experimental security analysis of a modern automobile.”
6. Theyazn H. H. Aldhyani , Hasan Alkahtani “Attacks to Automatous Vehicles A Deep Learning Algorithm for Cybersecurity”
7. Chen Dong , Hao Wu , and Qingyuan Li “Multiple Observation HMM-Based CAN Bus Intrusion Detection System for In-Vehicle Network“