**Otonom Araçlarda CAN Bus Üzerinden Saldırıların Analizi ve Yeni Bir Algılama Çözümü**

Bu makale, **CAN Bus protokolüne yönelik mevcut saldırıları analiz ederek yeni bir tespit yöntemi önermektedir.** Araştırmacılar, **Dacia Lodgy ve Sandero 2014 araçları üzerinde saldırı testleri yapmış** ve saldırıların nasıl gerçekleştirildiğini uygulamalı olarak göstermiştir. Son olarak, saldırıları **algılayan ve önleyen yeni bir yöntem** geliştirilmiştir.

**1. CAN Bus ve Güvenlik Açıkları**

**CAN Bus (Controller Area Network)**, **araç içindeki Elektronik Kontrol Üniteleri (ECU'lar) arasında haberleşmeyi sağlayan bir protokoldür.** Ancak, **şifreleme ve kimlik doğrulama mekanizmalarının eksikliği nedeniyle saldırılara karşı savunmasızdır.**

**CAN Bus'ın Güvenlik Açıkları**

* **Fiziksel veya Uzaktan Erişim Kolaylığı** → OBD-II portu veya kablosuz bağlantılar (Wi-Fi, Bluetooth) kullanılarak sızılabilir.
* **Şifreleme Eksikliği** → Mesajlar açık metin olarak gönderildiği için kötü niyetli kişiler trafiği dinleyebilir.
* **Kimlik Doğrulama Yok** → ECU’lar gönderilen mesajın kaynağını doğrulayamaz.
* **Trafik Kontrolünün Zayıflığı** → ECU’lar sürekli mesaj aldığı için saldırganlar sahte mesajlarla ağı manipüle edebilir.

📌 **Örnek:** Bir saldırgan, aracın fren sistemine sahte komutlar göndererek frenleri devre dışı bırakabilir.

**2. CAN Bus Üzerinden Gerçekleşen Saldırılar**

Makale, saldırıları **fiziksel erişim gerektiren** ve **uzaktan erişimle yapılan** saldırılar olarak ikiye ayırmaktadır.

**2.1. Fiziksel Saldırılar**

* **OBD-II Portu Üzerinden** → Araç içine fiziksel olarak erişerek doğrudan CAN Bus’a bağlanma.
* **ECU Manipülasyonu** → ECU’nun yazılımını değiştirerek sahte mesajlar üretme.
* **CAN Bus Ağına Harici Bir ECU Eklemek** → Sahte ECU’larla sistemi manipüle etme.

**2.2. Uzaktan Yapılan Saldırılar**

* **Kablosuz Bağlantılar Kullanarak Saldırı (Wi-Fi, 4G, Bluetooth)** → Araç içi sistemlere uzaktan erişim sağlanabilir.
* **Fuzzing (Bozuk Veri Gönderme)** → Rastgele mesajlar göndererek ECU’ların çökmesini sağlama.
* **Denial of Service (DoS) Saldırıları** → CAN Bus’a yüksek öncelikli mesajlar göndererek ağ trafiğini kilitleme.
* **ECU Spoofing (Kimlik Taklidi)** → Mevcut ECU’ları taklit ederek sahte mesajlar gönderme.

🚨 **Gerçek Örnekler:**  
1️⃣ **2015 Jeep Cherokee Hack Olayı** → Araç uzaktan hacklenerek direksiyon ve fren sistemleri kontrol edildi.  
2️⃣ **Candy Cream Saldırısı** → Araç içi bilgi-eğlence sistemi (IVI) üzerinden CAN Bus ağına sızılarak araç kontrol edildi.

**3. CAN Bus’a Yapılan Bir Saldırının Uygulamalı Gösterimi**

Makalede, bir **Dacia Lodgy 2014** üzerinde yapılan saldırı deneyleri anlatılmıştır.

**3.1. Saldırı Süreci**

1️⃣ **CAN Bus Üzerindeki Mesajları Dinleme (Sniffing)**

* OBD-II portuna bağlanarak CAN mesajları okunur.
* Mesajlardaki kimlikler (ID) belirlenerek hangi ECU’nun neye tepki verdiği analiz edilir.

2️⃣ **Kritik Mesajların Tespiti**

* Örneğin, **RPM bilgisini içeren mesajlar** belirlenir (ID: 0x186).
* Direksiyon, sinyaller, hız gibi sistemlerin mesajları ayrıştırılır.

3️⃣ **Sahte Mesaj Gönderme (Spoofing ve Injection)**

* Saldırgan, **CAN Bus’a sahte mesajlar enjekte eder** ve sistemleri manipüle eder.
* **Örnek:** ID 0x186’ya sahte RPM verileri girilerek gösterge panelinde yanlış hız gösterimi sağlanır.

📌 **Sonuç:** Araç içi sistemler **yanıltılarak** hatalı bilgi göstermeye zorlanmıştır.

**4. Saldırıları Önleme: Yeni Bir Algılama Mekanizması (IDS - Intrusion Detection System)**

Makalede, saldırıları önlemek için **"Frekans Tabanlı Saldırı Tespit Sistemi" (Frequency-Based IDS)** önerilmektedir.

**4.1. IDS Nasıl Çalışır?**

1️⃣ **CAN mesajlarının frekansı analiz edilir.**  
2️⃣ **Gerçek ECU’ların gönderdiği mesajlarla saldırganın gönderdiği mesajlar kıyaslanır.**  
3️⃣ **Anormal mesaj frekansları tespit edilirse, saldırı algılanır.**

**📌 Örnek:**

* Gerçek bir ECU **saniyede 5 mesaj** gönderirken, saldırgan **saniyede 50 mesaj** enjekte ederse, IDS bu anormalliği fark eder.
* Eğer **sahte mesajların zamanlaması, gerçek mesajlardan önce geliyorsa**, sistem saldırıyı tespit eder ve alarm verir.

**4.2. IDS Algoritmasının Güçlü ve Zayıf Yönleri**

| **Avantajlar** | **Dezavantajlar** |
| --- | --- |
| ✅ Gerçek zamanlı saldırı tespiti | ❌ Bazı gelişmiş saldırıları algılamak zor olabilir |
| ✅ Mevcut CAN sistemlerine kolay entegre edilebilir | ❌ Yanlış pozitif oranı yüksek olabilir |
| ✅ Şifreleme gerektirmez, ek işlem yükü düşüktür | ❌ Saldırgan mesaj gönderme hızını değiştirerek tespitten kaçabilir |

📌 **Öneri:** IDS sistemi **şifreleme (AES-128) ve makine öğrenmesi tabanlı sistemlerle desteklenmelidir.**

**5. SONUÇLAR ve ÖNERİLER**

1️⃣ **CAN Bus Protokolü Ciddi Güvenlik Açıklarına Sahiptir.**

* Şifreleme ve kimlik doğrulama eksikliği nedeniyle saldırılar kolayca gerçekleştirilebilir.

2️⃣ **Gerçek Araçlar Üzerinde Yapılan Testlerde, CAN Bus’un Manipüle Edilebildiği Gösterilmiştir.**

* OBD-II portu kullanılarak sahte mesajlar enjekte edilmiş ve araç içi sistemler yanıltılmıştır.

3️⃣ **Yeni Geliştirilen IDS Algoritması, Mesaj Frekanslarını Analiz Ederek Saldırıları Algılamaktadır.**

* Ancak, **tek başına yetersiz olabilir**, bu nedenle **kriptografik çözümlerle birleştirilmelidir.**

📌 **Teziniz İçin Çıkarımlar:**

* **Gerçek araçlar üzerinde saldırı simülasyonları yapabilirsiniz.**
* **IDS ve makine öğrenmesi tabanlı saldırı tespit sistemlerini kıyaslayabilirsiniz.**
* **Otonom araçlarda CAN Bus güvenliğini artırmak için hibrit çözümler önerebilirsiniz.**

Bu çalışmayı teziniz için kullanarak, **CAN Bus saldırılarına karşı savunma yöntemlerini deneysel olarak test edebilir ve yeni güvenlik algoritmaları geliştirebilirsiniz.** 🚗💻