**Detaylı Analiz: CAN Bus Saldırıları ve Güvenlik Çözümleri Üzerine Üç Makale İncelemesi**

Bu doküman, aşağıdaki üç çalışmanın detaylı analizini içermektedir:

1. **“Analyzing the CAN Protocol Vulnerabilities, Protective Measures and Improvements”**
   * **Yazarlar:** Mahender Reddy Bobbala ve Dr. R. Kavitha
2. **“Prevention of Controller Area Network (CAN) Attacks on Electric Autonomous Vehicles”**
   * **Yazarlar:** Salah Adly, Ahmed Moro, Sherif Hammad, Shady A. Maged
3. **“Analysis of current attacks on the CAN bus and development of a new solution to detect these types of malicious threats”**
   * **Yazarlar:** Mohammed Karrouchi ve arkadaşları

Bu analiz, hem CAN protokolünün zayıf yönlerini hem de mevcut saldırı senaryolarını ve bu saldırılara karşı önerilen çözümleri detaylandırarak, teziniz için kapsamlı bir referans kaynağı sunmaktadır.

**1. Giriş ve Temel Kavramlar**

**1.1. CAN Bus Protokolü**

* **Tanım:**  
  CAN (Controller Area Network) protokolü, modern araçlarda ECU’lar (Elektronik Kontrol Üniteleri) arasındaki veri iletişimini sağlar.
* **Özellikler:**
  + Yayın tabanlı (broadcast) yapı
  + Gerçek zamanlı iletişim (maksimum 1 Mbps)
  + Düşük kablolama karmaşıklığı ve EMI dayanıklılığı

**1.2. Güvenlik Zafiyetleri**

* **Şifreleme Eksikliği:**  
  Mesajlar açık metin olarak iletilir.
* **Kimlik Doğrulama Yetersizliği:**  
  ECU’lar arasında mesajın kaynağı doğrulanamaz.
* **Ağ Segmentasyonu Eksikliği:**  
  Tek bir ECU’ya erişim sağlandığında tüm ağa sızılabilir.

Bu temel kavramlar, analiz edilen makalelerin ortak noktalarını oluşturmakta ve her üç çalışma da bu güvenlik açıklarının araç güvenliği üzerindeki potansiyel etkisini ortaya koymaktadır.

**2. Makale 1: “Analyzing the CAN Protocol Vulnerabilities, Protective Measures and Improvements”**

**2.1. Temel Bulgular**

* **Zayıflıklar:**
  + CAN protokolü, şifreleme, kimlik doğrulama ve bütünlük kontrolleri içermediğinden, mesaj enjeksiyonu, DoS (Hizmet Reddi) ve sahte ECU kimliklendirmesi gibi saldırılara açıktır.
* **Çözüm Önerileri:**
  + Ağ bölümlendirme (network segmentation)
  + Şifreleme ve kimlik doğrulama tekniklerinin entegrasyonu
  + Makine öğrenmesi tabanlı IDS (Intrusion Detection System) uygulamaları

**2.2. Uygulamalı Örnekler**

* **Mesaj Enjeksiyonu Saldırıları:**  
  Bir saldırgan, ECU’lar arasında sahte mesajlar göndererek aracın fren veya hızlanma sistemini etkileyebilir.
* **IDS Sistemleri:**  
  Random Forest, SVM, DNN gibi algoritmalar kullanılarak anormal CAN trafiği tespit edilmiştir. Ancak, bilinmeyen saldırıları yakalamada sınırlamalar bulunmuştur.

**2.3. Değerlendirme**

Makale, CAN protokolünün tarihsel olarak güvenlikye odaklanmadan geliştirildiğini, ancak modern araçlarda artan ECU sayısı ve bağlantılı sistemler nedeniyle bu eksikliklerin giderek daha kritik hale geldiğini vurgulamaktadır. Çözüm önerileri, hem ağ düzeyinde hem de ECU düzeyinde uygulanabilecek yöntemlere odaklanmaktadır.

**3. Makale 2: “Prevention of Controller Area Network (CAN) Attacks on Electric Autonomous Vehicles”**

**3.1. Temel Bulgular**

* **Artan Bağlantılılık ve Güvenlik Riskleri:**  
  Otonom araçlarda, daha fazla ECU ve dış bağlantı (IoT, OTA güncellemeleri) CAN Bus’ın saldırıya açık hale gelmesine neden olmaktadır.
* **Önerilen Güvenlik Çözümü – Secure Boot:**
  + ECU’ların başlatılması sırasında yazılımın kriptografik bütünlüğünün kontrolü.
  + Böylece, kötü amaçlı kod içeren ECU’ların çalıştırılması engellenir.
* **Testler ve Performans Ölçümleri:**
  + Farklı veri bütünlüğü algoritmaları (CMAC, ECDSA, HMAC, RSA-PSS) test edilmiş ve CMAC ile ECDSA’nın belirgin avantajları ortaya konmuştur.
  + Özellikle, **ECDSA-CMAC** algoritması %19 performans artışı sunarak öne çıkmıştır.

**3.2. Uygulamalı Örnekler**

* **Secure Boot Uygulaması:**  
  ECU başlatma sürecinde, yazılımın hash değeri hesaplanır ve depolanmış referans değeri ile karşılaştırılır.
* **Örnek Saldırı Senaryosu:**  
  Uzaktan kötü amaçlı kod enjeksiyonu yoluyla bir ECU’nun kontrolü ele geçirildiğinde, Secure Boot mekanizması sayesinde kötü amaçlı yazılım çalıştırılamaz.

**3.3. Değerlendirme**

Bu makale, geleneksel kriptografik yöntemlerin (AES-128, HMAC, vb.) ek yük getirdiğini ancak Secure Boot’un ECU seviyesinde saldırıların temel nedenine (kötü amaçlı kod) müdahale edebileceğini göstermektedir. Ayrıca, test sonuçları ve performans değerlendirmeleri, farklı algoritmaların avantajlarını net bir şekilde ortaya koymaktadır.

**4. Makale 3: “Analysis of current attacks on the CAN bus and development of a new solution to detect these types of malicious threats”**

**4.1. Temel Bulgular**

* **Saldırı Senaryoları ve Deneysel Çalışmalar:**
  + Makalede, hem fiziksel hem de uzaktan yapılan saldırı örnekleri üzerinde detaylı deneysel çalışmalar yer almaktadır.
  + Özellikle, **OBD-II portu üzerinden yapılan fiziksel saldırılar** ve CAN Bus’a sahte mesaj enjeksiyonu örnekleri ayrıntılı olarak sunulmuştur.
* **Önerilen Algılama Yöntemi – Frekans Tabanlı IDS:**
  + CAN mesajlarının gönderilme sıklığı (frekansı) analiz edilerek, normal ECU trafiğinden sapmalar tespit ediliyor.
  + Anormal mesaj gönderme frekansı, IDS tarafından saldırı olarak işaretleniyor.

**4.2. Uygulamalı Örnekler**

* **Fiziksel Saldırı Deneyleri:**
  + Deneysel aşamada, bir aracın CAN mesajları gerçek zamanlı olarak dinlenmiş ve belirli mesaj ID’lerinin (örneğin 0x186 – RPM bilgisi) hangi ECU tarafından kontrol edildiği tespit edilmiştir.
  + Daha sonra, aynı ID ile sahte mesajlar enjekte edilerek aracın gösterge panelinde hatalı bilgi üretildiği gözlemlenmiştir.
* **IDS Tespiti:**
  + Gerçek ECU’nun belirli frekansta gönderdiği mesajlarla saldırganın yüksek frekansta enjekte ettiği mesajlar arasında zaman farkı bulunması, IDS algoritması ile tespit edilebilmiştir.

**4.3. Değerlendirme**

Makalede, CAN Bus saldırılarının pratikte nasıl gerçekleştirilebildiği detaylı bir şekilde gösterilmiştir. Frekans analizi temelli IDS sistemi, özellikle düşük veri işleme yükü ve gerçek zamanlı tespit imkanı sunması bakımından öne çıkmaktadır. Bununla birlikte, bazı durumlarda saldırganın gönderme hızını ayarlayarak tespit mekanizmasını atlatabilme riski de mevcuttur; bu nedenle, sistemin diğer kriptografik önlemlerle desteklenmesi önerilmektedir.

**5. Karşılaştırma ve Sentez**

**5.1. Ortak Bulgular**

* **CAN Bus’ın Doğasından Kaynaklanan Güvenlik Zayıflıkları:**  
  Üç makale de, CAN Bus’ın temel olarak şifreleme, kimlik doğrulama ve ağ segmentasyonu eksikliği nedeniyle saldırılara açık olduğunu ortaya koymaktadır.
* **Saldırı Türleri:**  
  Mesaj enjeksiyonu, DoS, ECU spoofing, ve fiziksel/uzaktan erişim gibi saldırı senaryoları tüm çalışmalarda tartışılmıştır.
* **Güvenlik Çözümleri:**
  + Makale 1: Ağ bölümlendirme, kriptografik önlemler, ve makine öğrenmesi tabanlı IDS.
  + Makale 2: ECU seviyesinde Secure Boot mekanizması ve farklı veri bütünlüğü algoritmalarının test edilmesi.
  + Makale 3: Frekans tabanlı IDS ile gerçek zamanlı saldırı tespiti ve ek deneysel saldırı simülasyonları.

**5.2. Farklı Yaklaşımlar**

* **Uygulama Seviyesi vs. ECU Seviyesi Çözümler:**  
  Makale 1 daha çok genel güvenlik önlemlerine odaklanırken, Makale 2 ECU’nun başlatılma sürecine müdahale ederek Secure Boot yaklaşımını sunmaktadır.
* **IDS Yöntemleri:**  
  Makale 3, CAN mesajlarının frekans analizine dayalı hafif IDS yöntemini ön plana çıkararak gerçek zamanlı tespit mekanizmasına dikkat çekmektedir.

**5.3. Teziniz İçin Öneriler**

* **Hibrit Yaklaşım:**  
  Üç çalışmanın bulguları, **Secure Boot, kriptografik yöntemler ve makine öğrenmesi tabanlı IDS sistemlerinin** bir arada kullanılması gerektiğini ortaya koymaktadır. Böylece, hem ECU düzeyinde kötü amaçlı kodların çalışması engellenebilir hem de CAN Bus trafiğinde anormallikler tespit edilebilir.
* **Deneysel Çalışmalar:**  
  Tezinizde, gerçek araçlar veya simülasyon ortamlarında, CAN Bus’a yönelik saldırı senaryoları (örneğin, OBD-II üzerinden mesaj enjeksiyonu) ve IDS algoritmalarının performans karşılaştırmalarını yapabilirsiniz.
* **Algoritma Performans Karşılaştırmaları:**  
  Makale 2’de test edilen farklı veri bütünlüğü algoritmalarının (CMAC, ECDSA, HMAC, RSA-PSS ve ECDSA-CMAC) hız ve güvenlik açısından karşılaştırılması, kendi deneysel çalışmalarınız için önemli bir referans noktası olabilir.
* **Geleceğe Yönelik Gelişim:**  
  Gelişen teknolojiler (örneğin, post-kuantum kriptografi) ve IoT entegrasyonunun araç güvenliği üzerindeki etkileri de tartışılabilir.

**6. Sonuç ve Gelecek Çalışmalara Yönelik Öneriler**

* **Güvenlik Açıklarının Kapsamlı Değerlendirilmesi:**  
  CAN Bus’ın yapısal eksiklikleri nedeniyle, araçlarda uygulanan tüm güvenlik önlemlerinin çok katmanlı (defense in depth) yaklaşım ile ele alınması gerekmektedir.
* **Hibrit Güvenlik Çözümleri:**  
  Secure Boot’un ECU seviyesinde uygulanması, IDS sistemlerinin gerçek zamanlı tespit yetenekleriyle birleştirilerek saldırıların etkisi minimize edilebilir.
* **Deneysel ve Simülasyon Çalışmaları:**  
  Farklı saldırı senaryoları ve IDS/kriptografik algoritmalarının performans analizleri, gelecekteki güvenlik protokollerinin geliştirilmesinde yol gösterici olacaktır.
* **Tez Çalışmanızda Derinlemesine İnceleme:**  
  Üç makaleden elde edilen bulguları sentezleyerek, özellikle otonom araçlarda CAN Bus güvenliğini artırmaya yönelik yeni yaklaşımlar geliştirebilir, ayrıca bu yaklaşımların hem pratik uygulanabilirliğini hem de performansını deneysel olarak doğrulayabilirsiniz.

**Sonuç**

Bu doküman, üç farklı makalenin detaylı analizine dayanmaktadır ve her biri CAN Bus protokolü üzerindeki saldırı türlerini, deneysel uygulamaları ve güvenlik çözümlerini farklı açılardan ele almaktadır. Teziniz kapsamında bu analizler, hem mevcut yaklaşımların eksik yönlerini hem de potansiyel hibrit çözümler geliştirme fırsatlarını ortaya koymaktadır. Bu sayede, otonom araçlarda siber güvenliğin artırılması için daha kapsamlı ve çok katmanlı bir güvenlik mimarisi oluşturulabilir.

Bu doküman, teziniz için detaylı ve anlaşılır bir temel oluşturarak, CAN Bus saldırıları ve güvenlik çözümleri üzerine derinlemesine çalışmanıza yardımcı olacaktır. Her bölümde yer alan örnekler ve öneriler, deneysel çalışmalarınızı yönlendirecek niteliktedir.