Üniversite	**:**	**T.C. İstanbul Kültür Üniversitesi**
Enstitüsü	**:**	**Lisansüstü Eğitim Enstitüsü**
Anabilim Dalı	**:**	**Bilgisayar Mühendisliği**
Program	**:**	**Bilgisayar Mühendisliği**
Tez Danışmanı	**:**	**Prof. Dr. Özgür Koray ŞAHİNGÖZ**
Tez Türü ve Tarihi	**:**	**Yüksek Lisans – Nisan 2022**

ÖZET

ARAÇ İÇİ AĞLARDA MAKİNE ÖĞRENİMİ TABANLI SALDIRI TESPİT SİSTEMİ

Gelişen dünyaya paralel olarak ulaşım teknolojileri de her geçen yıl önemli ölçüde gelişmeye ve değişmeye başlamıştır. Bu gelişim süreci ile beraber belli başlı sorunlar da kendini göstermeye başlamıştır. İvmeli olarak yükselen insan nüfusu ve aynı ivme ile artan ulaşım ihtiyaçları, toplu yaşam alanlarında araç kazalarında artışa neden olmaktadır. Buna ek olarak trafik sorunları ve yakıt tüketimi artışı sorunları da kendini göstermektedir. Bu döngünün getirdiği sorunların yeni teknolojik kazanımların kullanımıyla çözülmesi gerektiği açıktır. Bu bağlamda, sürücüsüz araçlar veya diğer adıyla otonom araçlar konseptleri iyi bir çözüm niteliği taşımaktadır. Her çözüm kendi sorunları da beraberinde getirmektedir. Bu çözüm de beraberinde belli başlı sorunları ortaya çıkarmaktadır. Günümüzde birçok otomobil, iki aşamada incelenen dijital güvenlik yaklaşımları ile geliştirilmektedir. Bu sistemler, dış kaynaklı siber saldırılardan koruma sağlamak için gereken bir tür gömülü sistem haberleşmesi (Denetleyici Alan Ağı (CAN) gibi) kullanılarak, araç içindeki ağda oluşturulur. Bu saldırılar, kural odaklı, anomali odaklı, liste odaklı sistemler vb. gibi çeşitli yollarla tespit edilebilir. Mevcut literatür, araştırmacıların bu tür saldırıların tespiti için bazı yapay zekâ tekniklerinin kullanımına odaklandığını göstermiştir. Yapılan çalışmada CAN güvenliği için makine öğrenimi yöntemlerine dayalı bir siber saldırı tespit sistemi önerilmiştir. Sonuç olarak, karar ağacı temelli toplu öğrenme modellerinin test edilen algoritmalar içerisinde en yüksek başarımı verdiği gözlemlenmiştir.

Anahtar Kelimeler: makine öğrenimi, saldırı tespit sistemi, CAN, akıllı araç

University : **T.C. İstanbul Kültür University**
Institute : **Institute of Graduate Studies**
Department : **Computer Engineering**
Program : **Computer Engineering**
Thesis Advisor : **Prof. Dr. Özgür Koray ŞAHİNGÖZ**
Degree Awerded And Date : **MS – APRIL 2022**

ABSTRACT

MACHINE LEARNING BASED INTRUSION DETECTION FOR IN-VEHICLE NETWORKS

Parallel with the developing world, transportation technologies have started to expand and change significantly year by year. This change brings with it some inevitable problems. Increasing human population and growing transportation-needs result many accidents in urban and rural areas, and this recursively results extra traffic problems and fuel consumption. It is obvious that the issues brought by this spiral loop needed to be solved with the use of some new technological achievements. In this context, self-driving cars or automated vehicles concepts are seen as a good solution. However, this also brings some additional problems with it. Currently many cars are provided with some digital security systems, which are examined in two phases, internal and external. These systems are constructed in the car by using some type of embedded system communication (such as the Controller Area Network (CAN)) which are needed to be protected from outsider cyberattacks. These attacks can be detected by several ways such as rule based system, anomaly based systems, list based systems, etc. The current literature showed that researchers focused on the use of some artificial intelligence techniques for the detection of this type of attack. In this study, an intrusion detection system based on machine learning is proposed for the CAN security, which is the in-vehicle communication structure. As a result of the study, it has been observed that the decision tree-based ensemble learning models results the best performance in the tested models. Additionally, all models have a very good accuracy level.

Keywords: machine learning, intrusion detection system, CAN, smart car