POLİTEKNİK DERGİSİ

JOURNAL of POLYTECHNIC

ISSN: 1302-0900 (PRINT), ISSN: 2147-9429 (ONLINE)
URL: http://dergipark.org.tr/politeknik

Endüstriyel kontrol sistemlerine (scada) yönelik siber terör saldırı analizi

Cyber terror attack analysis for industrial control systems (scada)

***Yazar(lar) (Author(s))**: Esra SÖĞÜT[1], O. Ayhan ERDEM[2]*

ORCID[1]: 0000-0002-0051-2271

ORCID[2]: 0000-0001-7761-1078

Bu makaleye şu şekilde atıfta bulunabilirsiniz(To cite to this article): Söğüt E., Erdem O. A.," Endüstriyel kontrol sistemlerine (scada) yönelik siber terör saldırı analizi", ***Politeknik Dergisi***, 23(2): 557-566, (2020).

Erişim linki (To link to this article): http://dergipark.org.tr/politeknik/archive

DOI: **10.2339/politeknik.562570**

Endüstriyel Kontrol Sistemlerine (SCADA) Yönelik Siber Terör Saldırı Analizi

Araştırma Makalesi / Research Article

Esra SÖĞÜT , O. Ayhan ERDEM*
Teknoloji Fakültesi, Bilgisayar Mühendisliği Bölümü , Gazi Üniversitesi, Ankara, Türkiye
(Geliş/Received : 09.05.2019 ; Kabul/Accepted : 31.07.2019)

ÖZ

Denetleyici Kontrol ve Veri Toplama Sistemleri veya Endüstriyel Kontrol Sistemleri, önemli görülen kritik altyapıların kontrolünü sağlayan sistemlerdir. Kritik altyapılara yönelik gerçekleştirilen ataklar, siber terör atakları olarak değerlendirilir. Bu kritik altyapıların siber terör ataklarına karşı güvenliğinin sağlanması ve işleyişinin devamlılığı büyük önem arz etmektedir. Bu çalışmada kritik altyapılardan gaz boru hattı kontrol sistemine ait bir veri kümesi kullanılmaktadır. Veri kümesinde, mevcut SCADA protokollerinden Modbus protokolüne yönelik Command Injection, Reconnaissance and DoS (Denial of Service) gibi kategorilerde çeşitli ataklar gerçekleştirilmiştir. Böylece atak uygulanan ve atak uygulanmayan durumların sahip olduğu davranışların incelenmesi, değerlendirilmesi ve atak tespitinin yapılabilmesi hedeflenmektedir. Bunun için veri kümesi üzerinde çeşitli algoritmalar ile veri madenciliği yöntemi kullanılmıştır. Elde edilen analiz sonuçlarına göre en doğru sınıflandırma oranının Random Tree algoritması ile sağlandığı görülmüştür. Bu algoritmaya ait analiz sonuçları incelenerek siber terör atak davranışları belirlenmiş ve böylece siber terör atak tespitinin gerçekleştirilmesi için ilgili alana önemli bir katkı sunulmuştur. Denetleyici Kontrol ve Veri Toplama Sistemlerinin veya Endüstriyel Kontrol Sistemlerinin siber güvenliğinin sağlanması için bu tür çalışmaların daha fazla yapılması ve yeni veri kümelerinin üretilerek kullanıma sunulması gerekmektedir.

Anahtar Kelimeler: Scada, eks, modbus, siber terör, siber saldırı.

Cyber Terror Attack Analysis for Industrial Control Systems (SCADA)

ABSTRACT

Supervisory Control and Data Acquisition Systems or Industrial Control Systems are the systems that control the critical infrastructures that are considered important. Attacks against critical infrastructures are considered as cyber terror attacks. Continuity of the operation of these critical infrastructures and ensuring the security of these critical infrastructures against cyber terror attacks are great importance. In this study, a data set of the gas pipeline control system, which is one of the critical infrastructures, is used. In the data set, several attacks were performed in the categories such as command injection, reconnaissance and denial of service for Modbus protocol which is one of the existing SCADA protocols. In this way, it is aimed to investigate and evaluate the behaviors of attacked and non-attacked situations. In addition, it is aimed to detect the attack. For this purpose, data mining method has been used with various algorithms on the data set. According to the analysis results, the most accurate classification rate is provided by Random Tree algorithm. By analyzing the results of this algorithm, cyber terror attack behaviors were determined and thus, an important contribution was made to the field of cyber terror attacks. In order to ensure cyber security of Supervisory Control and Data Acquisition Systems or Industrial Control Systems, such studies need to be carried out further and new data sets should be produced and put into use.

Keywords: Scada, ics, modbus, cyber terror, cyber attack.

1. GİRİŞ (INTRODUCTION)

Denetleyici Kontrol ve Veri Toplama Sistemleri/ Supervisory Control and Data Acquisition (SCADA) veya Endüstriyel Kontrol Sistemleri
(EKS), kritik altyapı olarak kabul edilen birçok sistemi izler ve kontrol eder. Elektrik, su, gaz gibi kaynakların üretimi, iletimi ve dağıtımı için oluşturulan sistemler kritik altyapılar olarak kullanılmaktadır. Ayrıca, Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'na (Türkiye) göre "Ulaşım, enerji, haberleşme, finans, sağlık, su yönetimi, kritik kamu hizmetleri" gibi yapılar da kritik altyapılar olarak belirlenmiştir [1].

Gelişen teknolojiye bağlı olarak kritik altyapılarda kullanılan SCADA veya EKS'ler de gelişmekte ve kullanım alanları artmaktadır. Kritik altyapılara yönelik gerçekleştirilen ataklar, sistemlerin çalışmasına zarar verebilir, işleyişi yavaşlatabilir, sistemi kısmen veya tamamen durdurabilir. Bu sistemlerin güvenliği öncelikli konular arasında yer almaktadır [2]. Bu şekilde meydana gelen ataklar, siber terör atakları olarak değerlendirilebilmektedir. Siber terör ataklarının yaşanması durumunda, kritik altyapı sistemleri hizmet edemez hale gelebilir ve bağlı bulunan diğer sistemler de olumsuz şekilde etkilenebilir. Ulusal ve uluslararası boyutlarda kullanılan bu sistemlerin güvenliği ve siber terör ataklarından korunması giderek önemli konular haline gelmektedir.

Yapılan çalışmalar incelendiğinde, Morris ve arkadaşlarının EKS için yeni bir siber atak veri kümesi oluşturduğu görülmüştür. Daha sonra, oluşturulan bu veri

*Sorumlu Yazar (Corresponding Author)
e-posta : ayerdem@gazi.edu.tr

kümesi genel kullanıma sunulmuştur [3]. Başka bir çalışmada, Shang ve arkadaşları EKS için saldırı tespit sistemlerini incelemiş ve sistemlerde kullanılan Modbus TCP haberleşmesi için yeni bir kural önermişlerdir [4]. Bhatia ve arkadaşları ise Modbus protokolünün saldırılara açık olduğunu belirtmiş ve saldırı tespit sistemlerine yönelik karşılaştırmalar yapmışlardır [5]. Hindy ve arkadaşları SCADA tarafından kontrol edilen bir su dağıtım sistemine ait veri kümesi üzerinde çalışarak belirledikleri ataklara karşı anomali tespitleri yapmışlardır. DoS, Spoofing veya algılayıcı arızaları gibi çeşitli ataklara göre senaryolar oluşturmuşlar ve anomali durumuna göre uyarı mekanizması geliştirmişlerdir [6]. Sugwon ve Myongho, SCADA için saldırı tespit sistemleri ile ilgili incelemeler yapmıştır. Sistemlerde anormal hareketlilik kontrolü için ağ trafiği desenlerinin oluşturulması gerektiğini söylemişlerdir [7]. Kang ve arkadaşları tarafından SCADA sistemlerine yönelik siber tehditler tartışılmış ve bu tehditler detaylandırılarak çizelge halinde sunulmuştur. Kimlik ihlali, zaman veya mantık bombaları, araya girme saldırıları, DoS, virüsler, terörizm, sabotaj, Spoofing gibi birçok tehdit çizelgede yer almaktadır [8]. Dell tarafından yayınlanan bir raporda ise SCADA'ya yönelik gerçekleştirilen saldırı metotlarına değinilmiştir. Buna göre komut enjeksiyonu, kodlar, çapraz-site istekleri, kriptoloji, izinler, yetkisiz alanlar, kaynak yönetimi gibi çeşitli metotlar SCADA'yı ilgilendirmektedir [9].

Deney düzeneği oluşturan Jung ve arkadaşları Modbus seri protokolü üzerinde çalışmışlardır. İç ağ yapısında Siniffing atağı gerçekleştirilmiş ve meydana gelen durum izlenmiştir. Bu atağa yol açan zafiyeti ortadan kaldırmak için pakete ait Rx ve Tx değerlerinin izlenmesinin gerekli olduğu belirtilmiştir [10]. Deney düzeneği kullanan başka bir çalışmada Korkmaz ve arkadaşları SCADA sisteminde bazı ataklar gerçekleştirerek statik ve dinamik veri elde edilebileceğini göstermişlerdir. Bu ataklar Man in the middle, Local DNS Poisoning, DoS, Malicious Software Injections, Firmware Modification Attack, Process Network Malware Injection ataklarıdır [11]. Başka bir deney düzeneği çalışmasında Hahn ve arkadaşları, SCADA protokollerinden olan DNP3 ve IEC 61850 protokolleri üzerindeki zafiyetlere odaklanmışlardır. Gereksiz port ve servis kullanımı, varsayılan hesap bilgilerinin güncellenmemesi gibi zafiyetler ele alınarak sisteme müdahale edilmiş ve başarılı olunmuştur. Bunun için rölenin yeniden yapılandırılması, DoS atağı, alarmlara müdahale edilmesi, yanlış alarm üretilmesi gibi ataklar gerçekleştirilmiştir. Varsayılan hesap bilgilerinin değiştirilmesi ve gereksiz şekilde açık bulunan portların kapatılması gerektiği vurgulanmıştır [12].

SCADA veya EKS'lere yönelik siber terör ataklarının incelenmesi tüm dünyada önem arz etmektedir. Özellikle kritik altyapıların siber terör ataklarından korunması, toplum yaşamının ve süreç işleyişlerinin kolaylıkla sürdürülebilirliği açısından vazgeçilemez hale gelmektedir. Yapılan çalışmalar incelendiğinde, SCADA veya EKS güvenliği için ataklar ele alınmış, saldırı tespit sistemleri incelenmiş, zafiyetler araştırılmış, çeşitli ataklar gerçekleştirilmiş ve sisteme müdahale etmek için deneyler yapılmıştır. Bu çalışmada ise veri kümesi üzerinde çeşitli algoritmalar kullanılarak veri madenciliği yapılacak ve atak davranışları analiz edilecektir. Ayrıca atak tespiti yapılmaya çalışılacak ve literatüre SCADA veya EKS odaklı siber terör ataklarından korunması için yeni bir bakış açısı sunulacaktır.

Çalışmada Morris ve arkadaşlarının oluşturduğu veri kümesi kullanılmaktadır [3]. Bu veri kümesi ile ilgili bilgiler dördüncü bölümde verilmektedir. Veri kümesi kullanılarak SCADA veya EKS'lere yönelik yapılan saldırılar farklı niteliklere göre değerlendirilip analiz edilmektedir. Bunun için Waikato Üniversitesi tarafından açık kaynak olarak dağıtılan ve Java ile geliştirilen bir veri madenciliği programı olan WEKA ile veri madenciliği yapılmaktadır. Veri madenciliğinde kullanılan ağaç tabanlı Decision Stump, Hoeffding Tree, J48, Random Tree ve REP Tree algoritmaları Çapraz Doğrulama (Cross-Validation) yöntemi ile analiz edilmektedir. Kullanılan algoritmalar ve veri madenciliği ile ilgili bilgiler dördüncü bölümde yer almaktadır. Bu algoritmalar atak yapılan ve yapılmayan veri kümesi üzerinde sınıflandırma yapmakta ve buna göre en doğru sınıflandırma oranı Random Tree algoritması (%84,0049) ile sağlanmaktadır. Elde edilen değerler analiz edilerek veri kümesi öznitelikleri arasında ilişkiler kurulmaktadır. Ayrıca siber güvenliğin sağlanması için çıkarımlarda bulunulmaktadır. SCADA veya EKS'ler için siber güvenliğin sağlanmasına yönelik yol gösterici bir çalışma yapılması hedeflenmektedir.

Çalışma altı bölümden oluşmaktadır. İlk bölümde genel bilgilerin ve daha önce yapılan çalışmaların sunulduğu giriş bulunmaktadır. İkinci bölümde siber terör ve üçüncü bölümde SCADA sistemleri hakkında bilgiler verilmektedir. Sonraki bölümde çalışmanın metodolojisi hakkında bilgiler verilmektedir. Beşinci bölümde gerçekleştirilen analiz hakkında bilgiler verilmektedir. Diğer bölümde ise elde edilen deneysel sonuçlar sunulmaktadır. Son bölümde sonuç yer almaktadır.

2. SİBER TERÖR VE SCADA SİSTEMLERİ (CYBER TERROR AND SCADA SYSTEMS)

Siber terör ve SCADA sistemleri bu bölümde ele alınmaktadır.

2.1. Siber Terör (Cyber Terror)

Terörist faaliyetlerinin gerçekleştirilmesi için siber dünyanın kullanılması, siber terör kavramının ortaya çıkmasını sağlamıştır. Siber terörün uluslararası alanda genel kabul gören bir tanımı yoktur. Genel olarak siber terör, kritik öneme sahip ulusal altyapılara (enerji, ulaşım, haberleşme gibi) bilgisayar ağlarını kullanarak zarar vermeyi veya bu altyapıları tamamen kullanılamaz hale getirmeyi amaçlayan saldırılar biçiminde kendini göstermektedir [13,14].

Siber terörün gerçekleştirme amaçları genel olarak devlet tarafından korunan telekomünikasyon, ulusal güvenlik ağları gibi yapılarda yer alan bilgilerin elde edilmesi,

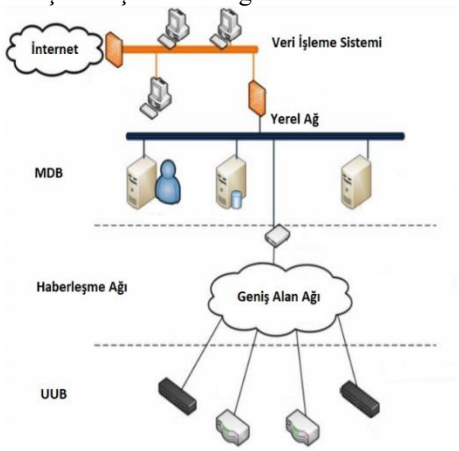
değiştirilmesi veya terörist eylemlerinde kullanılmasıdır. Ayrıca siber terör, siyasal bir amaç için insanlara zarar vermeyi veya acı çektirmeyi de hedeflemektedir. Geleneksel terörden farklı olarak siber terör bazı özelliklere sahiptir. Bunlar siber terör yöntemlerinin kullanılması, siber terör saldırısının gerçekleştirilme sebepleri, saldırıyı düzenleyenin bilinçli olarak bilgi teknolojilerini kullanması şeklinde sıralanabilir. Siber terör saldırıları, geleneksel terör saldırılarına göre daha ölümcül düzeyde tehlikeler taşıyabilmektedir [15,16].
Morris ve arkadaşlarının yaptığı çalışmada siber ataklar geliştirilmiş, gaz boru hattı kontrol sistemine bu ataklar uygulanmış ve sistemin tepkisine göre bir veri kümesi elde edilmiştir [3]. Gaz boru hattı gibi kritik altyapılara yönelik gerçekleşen ataklar siber terör atakları olarak kabul edilebilmektedir. Bu ataklar, çalışmada siber terör atakları olarak değerlendirilmekte ve veri madenciliği ile analiz edilmektedir.

2.2. SCADA Sistemleri (SCADA Systems)

SCADA veya EKS'ler kritik altyapıları izler ve denetler. Gaz boru hatları, enerji santralleri, demiryolları, su arıtma tesisleri ve daha birçok sistem kritik altyapı olarak değerlendirilmektedir. Bu sistemlerin çoğu geçmişte tüm ağlardan bağımsız ve izole edilmiş şekilde çalışmaktaydı. Son zamanlarda ise internet ve kurumsal ağlarla birlikte çalışır hale getirildi. Bu durum beraberinde güvenlik kaygılarını da getirmektedir. Bu sistemlerde bir güvenlik açığının olması sistemin uzaktan ele geçirilmesini ve kullanılmasını mümkün kılmaktadır. Böyle bir durum ise bireysel veya toplumsal olarak insanların hayatına zarar verebilecek sorunların ortaya çıkmasına sebep olabilir [17].
SCADA veya EKS'lerin sahip olduğu özelliklere bu bölümde değinilmektedir. Temel bileşenler ve kullanılan protokoller, siber güvenlik için dikkat edilmesi gereken konuları oluşturmaktadır.

2.2.1. Temel bileşenler (Basic components)

SCADA veya EKS temel bileşenleri 3 bölümden oluşmaktadır. Bunlar; Merkezi Denetleyici Birimi (MDB)/Master Terminal Unit, Uzak Uç Birimleri (UUB)/Remote Terminal Unit ve haberleşme ağıdır. Bu temel bileşenlere Veri İşleme Sistemi de eklenebilir. Bileşenler Şekil 1.'de gösterilmektedir.



Şekil 1. Temel bileşenler (Basic components) [18,19]

MDB, sistemdeki sunucuların veya bilgisayarların ana sunucuya bağlantı halinde olmasını ve haberleşmeyi sağlamaktadır. Grafiksel ara yüz bu bölümde bulunmaktadır. UUB'lerden gelen veriler toplanır ve ara yüzde bu veriler gösterilir. UUB ise sistem tarafından izlenen cihazlardan oluşmaktadır. Algılayıcıların ve modüllerin izlenmesi ve kontrol edilmesi bu bölümde gerçekleştirilmektedir. Programlanabilir Mantık Denetleyicileri (Programmable Logic Controller) bu bölümde yer almaktadır. Sistemde haberleşmeyi hızlandırmak ve daha akıllı UUB elde etmek için gerekli işlemlerin hepsi SCADA veya EKS haberleşme ağı üzerinden gerçekleştirilir. Haberleşme için radyo, telefon hattı, mikrodalga, uydu, kablo, fiber optik veya özel protokoller kullanılmaktadır [19-22].
Haberleşme ağı üzerinde Modbus protokolü kullanılarak üretilen veri kümesi çalışmada kullanılmaktadır [3].

2.2.2. Haberleşme protokolleri (Communication protocols)

SCADA veya EKS temel bileşenleri arasında iletişim sağlamak için özel haberleşme protokolleri kullanılmaktadır. En çok kullanılan haberleşme protokolleri şunlardır [17-20]:

- Modbus
- DNP3
- Profinet
- EthernetIP
- ControlNet
- Foundation Fieldbus
- Profibus

Çalışmada Modbus protokolü ile ilgili veriler kullanılmaktadır. Modbus, 1979 yılında tasarlanmış ve otomasyon alanında bir standart haline gelmiş bir haberleşme protokolüdür. İstemci-sunucu mimarisinde seri hat üzerinde çalışmakta ve iki katman içermektedir. Bu protokol geliştirilmekte ve birçok sistem tarafından desteklenmektedir. Modbus Seri ve Modbus TCP olarak iki farklı Modbus türü bulunmaktadır [18].

3. MATERYAL VE METOD (MATERIAL AND METHOD)

Bu çalışmada kullanılan veri kümesi, bir SCADA sistemine ait seri hat üzerindeki Modbus protokolünden alınmıştır. Bu veri kümesi, Morris ve arkadaşları tarafından gaz boru hattı kontrol sisteminden elde edilmiştir [3].
Veri kümesindeki her örnek, yük taşıma (payload) bilgileriyle birlikte ağ trafik bilgilerini de içerir. Ağ bilgisi, sisteme izinsiz giriş yapıldığında bunun tespiti için bir iletişim şekli sağlar. Bilgi teknolojileri ağlarının aksine, SCADA veya EKS'ler sabit ağ topolojilerine sahiptir ve düğümler arasındaki işlemler tekrarlı ve düzenlidir. Bu sabit davranış, anormal hareketliliği tespit etmek için atak tespit sistemlerine kolaylık sağlamaktadır. Yük taşıma bilgileri gaz boru hattının durumu, ayarları ve parametreleri hakkında bilgi sağlar. Bu değerler sistemin nasıl performans gösterdiğini

anlamak ve sistemin sınırlarını aşan durumları veya sistemin kritik bir durumda olup olmadığını tespit etmek için çok önemlidir [3,17].

3.1. Veri Kümesi (Data Set)

Veri kümesinde toplam 274,628 örnek vardır. Veri kümesindeki her satır, öznitelik olarak adlandırılan birden çok sütun içerir [3,17]. Veri kümesine ait 10 adet öznitelik ve atakların yer aldığı sonuç özniteliği bu çalışmada kullanılmaktadır. Çalışmada kullanılan öznitelikler ve her özniteliğe ait açıklamalar Çizelge 1'de gösterilmektedir. İlk öznitelik olan adres, Modbus köle cihazın istasyon adresini içerir. İstasyon adresi, her ana ve köle cihaza atanan benzersiz bir sekiz bitlik değerdir. Adres, yöneticinin komutları ilettiği köleyi ve yanıt veren köleyi tanımlamak için kullanılır. Modbus protokolü, tüm köle cihazların tüm ana işlemleri alacağı şekilde yapılandırılmıştır. İkinci öznitelik olan fonksiyon, fonksiyon kodunu içerir. Gaz boru hattında kullanılan fonksiyon kodları okuma ve yazma komutları olarak 256 farklı fonksiyon kodu olasılığı bulundurmaktadır. Bu durum kodların kötü amaçlı kullanımlarına sebep olabilmektedir.

Çizelge 1. Öznitelik listesi (Attribute list)

No	Öznitelik	Açıklama
1	adres	Modbus köle cihazının istasyon adresi (20 adet)
2	fonksiyon	Modbus fonksiyon kodu
3	uzunluk	Modbus çerçevesinin uzunluğu
4	kazanç	PID kazancı
5	devir süresi	PID devir süresi
6	sistem şıkları	Sistem şıkları; otomatik, manuel, kapalı
7	kontrol şeması	Kontrol şeması; pompa, solenoit
8	pompa	Pompa kontrolü; açık, kapalı
9	solenoit	Tahliye vanası kontrolü; açık, kapalı
10	komut yanıtı	Komut, cevap
11	sonuç	Atak sınıfları (8 adet)

Uzunluk özniteliği, Modbus çerçevesinin uzunluğunu gösterir. Fonksiyon koduna benzer şekilde, Modbus çerçevesinin uzunluğu her komut veya yanıt sorgusu için sabittir. Saldırı tespitinde, belirli bir uzunlukta olmayan çerçeveler kolayca anormal olarak algılanır.

Kazanç özniteliği ise PID (Proportional Integral Derivative, Oransal Integral Türevsel Denetleyici Kontrol Döngüsü) kontrol cihazını ayarlamak için kullanılan değerlerden biridir. Bu değere göre hesap yapılıp hata oranı saptanır. Bu oranı en aza indirmek için PID denetleyicisi, tahliye vanasını açar/kapatır veya pompayı açar/kapatır. Böylece kazanç elde edilmeye çalışılır.

Gaz boru hattı en düşük seviyede, basınç algılayıcısıyla birlikte pompa ve solenoit olarak iki çalıştırıcı içerir. Bunlar denetim kontrolleri tarafından ayarlanan basıncı korumak için ve sistemin fiziksel işlemini kontrol etmek için kullanılır. Pompa ve solenoit kontrolünde açık ve kapalı olarak iki fonksiyon vardır ve sadece manuel olarak çalışırlar.

Gaz boru hattının üç ana sistem şıkkı vardır: Otomatik, manuel, kapalı. Sistem otomatik şık üzerindeyken, denetleme kontrolleri tarafından karar verilen basıncı korumak için iki kontrol şeması vardır. İlki pompa şıkkıdır ve borudaki basıncı ayar noktasında tutmak için pompayı açıp kapatır. İkincisi, basıncı ayarlamak için bir tahliye vanasının açıldığı ve kapatıldığı solenoit şıkkıdır. Sistem şıkkı ayrıca operatörün pompayı ve solenoiti manuel olarak kontrol etmesini sağlayan manuel şık da olabilir.

Komut yanıtı özniteliği, bir atak tespit sisteminin komutlar ve cevaplar arasındaki farkı öğrenmesine izin vermek için kullanılmaktadır.

Bu veri kümesi hem normal durum (atak uygulanmayan) hem de farklı siber terör atak örneklerinin uygulandığı verileri içermektedir. Veri kümesinde 214580 adet atak uygulanmayan ve 60048 adet atak uygulanan örnekler bulunmaktadır. Sonuç olarak, sisteme karşı 7 farklı atak sınıfı geliştirilmiş ve bunlar uygulanmıştır. Bu 7 farklı atak sınıfları, normal sınıf ve bu sınıfların her birine ait örnek sayısı Çizelge 2'de yer almaktadır.

Çizelge 2. Atak sınıfları (Attack classes)

No	Atak Sınıfı	Örnek Sayısı
0	Normal	214580
1	Naive Malicious Response Injection (NMRI)	7753
2	Complex Malicious Response Injection (CMRI)	13035
3	Malicious State Command Injection (MSCI)	7900
4	Malicious Parameter Command Injection (MPCI)	20412
5	Malicious Function Code Injection (MFCI)	4898
6	Denial of Service (DoS)	2176
7	Reconnaissance (R)	3874

Command injection atakları, malicious state command injection (MSCI), malicious parameter command injection (MPCI) ve malicious function code injection (MFCI) ataklarını içerir.

Response injection atakları iki tür davranış gösterir. Birincisi, normal operasyonda bulunmayan ve kural dışı davranışa sahip olan naive malicious response injection (NMRI) atağıdır. Bu atak türü genellikle kötü niyetli saldırganların fiziksel sistem süreci hakkında bilgi sahibi olmadığında ortaya çıkar. İkincisi ise complex malicious response injection (CMRI) atağıdır. Bu atak türü, belirli

normal davranışları taklit eden saldırıları tasarlamak için durumu ve fiziksel süreç bilgilerini kullanır.

Bir sonraki atak kategorisi reconnaissance (R) atağıdır. Bu ataklar, pasif bilgi toplamak veya bir aygıttan sistem hakkındaki bilgiyi zorla almak için tasarlanmıştır. Elde edilecek bilgi, ağ bilgilerini (durum adresi, uzunluk vb.) veya cihaz özelliklerini (model numarası, iletişim protokolü, üretici vb.) içerebilir.

Denial of service (DoS) atakları, kontrol ve süreç arasındaki iletişimi engellemeye çalışır. Bu, kablosuz ağların kesilmesiyle veya ağ protokollerinin kötüye kullanılmasıyla yapılabilir.

3.2. Veri Madenciliği ve Karar Ağaçları (Data Mining and Decision Trees)

Veri madenciliği, var olan verinin işlenmesi ve kullanıma uygun olacak şekilde sonuçlar elde edilmesidir. Veri madenciliği ile farklı yöntemler kullanılarak farklı işlemler gerçekleştirilebilir. Veriye en uygun modeli sağlamak için farklı algoritmalar seçilir. Veri madenciliğinde kullanılan modeller tahmin edici ve tanımlayıcı modeller olarak iki grupta incelenmektedir [23,24].

Çalışmada veri madenciliği için WEKA kullanılmaktadır. Veri hazırlama, sınıflandırma, regresyon, kümeleme, birleşme kuralları madenciliği ve görselleştirme için çeşitli araçlar içerir [25]. WEKA, siber atak tespiti alanındaki birçok çalışmada belirli algoritmaların performansını test etmek için kullanılmaktadır [17].

Çalışmada tahmin edici modeller altında bulunan sınıflama yöntemine ait karar verici algoritmalardan ağaç tabanlı olanlar kullanılmaktadır. Karar Ağaçları olarak adlandırılan bu algoritmalar, siber atakların tespitinde sıklıkla kullanılmakta ve veri setleri üzerinde uygulanmaktadır. Bu sebeplerden dolayı çalışmada bu algoritmalar tercih edilmiştir. Decision Stump, Hoeffding Tree, J48, Random Tree ve REP Tree algoritmaları çalışmada kullanılmaktadır.

Veri kümesi üzerinde bu algoritmalar ile çalışılarak analizler yapılmaktadır. Atak olmayan ve atak olan durumların doğru sınıflandırılması için algoritmalar tek tek uygulanmaktadır. Yapılan analizlere göre her algoritma için sınıflandırma oranı elde edilmekte ve birbirine göre kıyaslamaları yapılmaktadır. Buna göre en doğru sınıflandırma oranına Random Tree algoritması sahip olmuştur. Bu oranlar Çizelge 3'te verilmektedir.

Çalışmada, en yüksek doğru sınıflandırma oranına sahip olan Random Tree algoritmasının analiz sonuçları üzerinde durulmaktadır. Bu algoritma analizine göre, düzensizlik matrisi elde edilmiş ve hesaplamalar yapılarak doğruluk yüzdesine ulaşılmıştır. Ayrıca, atak olmayan ve atak olan durumların diğer özniteliklere göre değişimleri de incelenmiştir. Elde edilen sonuçlar sunulmuştur.

4. ANALİZ (ANALYSIS)

Kullanılan algoritmalar ve elde edilen analiz sonuçlarına bu bölümde yer verilmektedir.

4.1. Algoritmaların Sınıflandırma Oranlarının Karşılaştırılması (Comparison of Algorithms and Classification Rates)

Veri analizi Decision Stump, Hoeffding Tree, J48, Radom Tree ve REP Tree algoritmaları Çapraz Doğrulama yöntemine göre uygulanmaktadır. Veri kümesi üzerinde uygulanan algoritmaların sınıflandırma yüzdelerinin ve sınıflandırma örnek sayılarının birbirlerine göre karşılaştırılmaları Çizelge 3'te gösterilmektedir.

Çizelge 3. Analiz sonuçları ve karşılaştırmalar (Analysis results and comparisons)

Algoritmalar	Doğru Sınıflandırılan Örnek Sayısı	Yanlış Sınıflandırılan Örnek Sayısı	Doğruluk Yüzdesi (%)
Decision Stump	214580	60048	78.1348
Hoeffding Tree	227065	47563	82.6809
Random Tree	**230701**	**43927**	**84.0049**
REP Tree	230391	44237	83.8920

Çalışmada, algoritma analizleri için sıklıkla kullanılan Çapraz Doğrulama yöntemi tercih edilmektedir. Bu yöntemde K katsayısı bulunmakta ve K-kere işlem geçekleştirilmektedir. Bu çalışmada K katsayısı 10 olarak seçilmektedir. Her adımda veri kümesinin 1/10'u kadar, daha önce test için kullanılmamış veri parçası test için kullanılmaktadır. Geri kalan kısmı ise eğitim için kullanılmaktadır. Böylece 10 defa farklı test kümesi olacak şekilde eğitim ve sınıflandırma işlemi gerçekleşecektir. Algoritmalar bu yönteme göre analiz edilmiş ve elde edilen sonuçlar birbirlerine göre kıyaslanmıştır. Buna göre sınıflandırma doğruluk oranının en yüksek olduğu algoritma Random Tree algoritması olarak belirlenmiştir.

4.2. Random Tree Algoritması İçin Düzensizlik Matrisi (Irregularity Matrix for Random Tree Algorithm)

Algoritma analiz sonuçlarında elde edilen düzensizlik matrisi Şekil 2.'de gösterilmektedir.

a	b	c	d	e	f	g	h	<-- classified as
213900	0	0	153	480	0	47	0	a = 0
7753	0	0	0	0	0	0	0	b = 1
13035	0	0	0	0	0	0	0	c = 2
5286	0	0	2534	78	0	2	0	d = 3
14974	0	0	23	5409	0	6	0	e = 4
0	0	0	0	0	4898	0	0	f = 5
1948	0	0	15	15	0	198	0	g = 6
40	0	0	0	0	72	0	3762	h = 7

Şekil 2. Random Tree algoritması için düzensizlik matrisi (The irregularity matrix for the random tree algorithm)

Şekil 2'de atak sınıflarına harfler verilerek matris oluşturulmuştur. Buna göre;

a. Normal durum (atak yaşanmayan)
b. NMRI atağının uygulandığı durum
c. CMRI atağının uygulandığı durum
d. MSCI atağının uygulandığı durum
e. MPCI atağının uygulandığı durum
f. MFCI atağının uygulandığı durum
g. DoS atağının uygulandığı durum
h. R atağının uygulandığı durumlar gösterilmektedir.

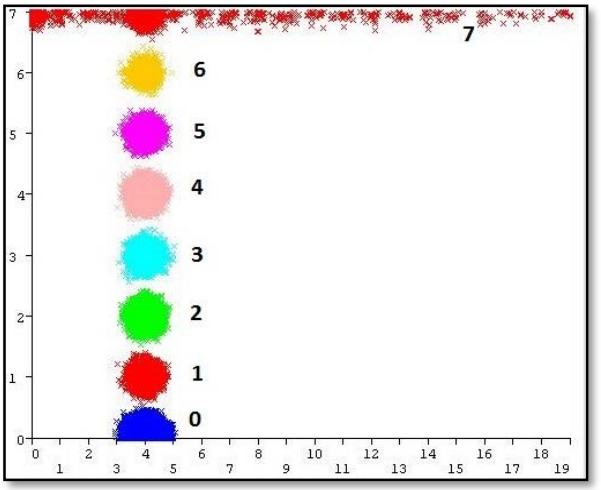
Şekil 2'ye göre;
214580 adet "normal" değerli test verisinin 213900 tanesi "normal", 153 tanesi "MSCI", 480 tanesi "MPCI" ve 47 tanesi "DoS" olarak tahmin edilmiştir.
7753 adet "NMRI" değerli test verisinin hepsi "normal" olarak tahmin edilmiştir.
13035 adet "CMRI" değerli test verisinin hepsi "normal" olarak tahmin edilmiştir.
7900 adet "MSCI" değerli test verisinin 5286 tanesi "normal", 2534 tanesi "MSCI", 78 tanesi "MPCI", 2 tanesi "DoS" olarak tahmin edilmiştir.
20412 adet "MPCI" değerli test verisinin 14974 tanesi "normal", 23 tanesi "MSCI", 5409 tanesi "MPCI", 6 tanesi "DoS" olarak tahmin edilmiştir.
4989 adet "MFCI" değerli test verisinin hepsi "MFCI" olarak tahmin edilmiştir.
2176 adet "DoS" değerli test verisinin 1948 tanesi "normal", 15 tanesi "MSCI", 15 tanesi "MPCI", 198 tanesi "DoS" olarak tahmin edilmiştir.
3874 adet "R" değerli test verisinin 40 tanesi "normal", 72 tanesi "MFCI", 3762 tanesi "R" olarak tahmin edilmiştir.

4.3. Random Tree Algoritması İçin Doğruluk Yüzdesi (Accuracy Percentage for Random Tree Algorithm)

Düzensizlik matrisine göre;
213900+2534+5409+4898+198+3762=230701 adet veri Random Tree algoritması ile oluşturulan modele göre doğru sınıflandırılmıştır.
78+23+40 =141 adet veri yanlış sınıflandırılmıştır.
Buna göre doğruluk sınıflandırma yüzdesi Eş.1'deki gibi hesaplanmıştır;
Doğruluk yüzdesi = 230701/[230701+(7753+ 13035+ 5286+14978+194+40+153+480+47+78+2+23+6+15+15+72)]x100=%84,0049 (1)

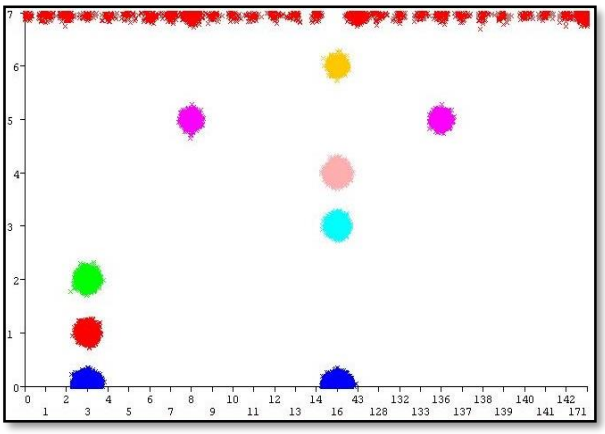
4.4. Random Tree Algoritması İçin Özniteliklerin Değerlendirilmesi (Evaluation of Attributes for the Random Tree Algorithm)

Random Tree algoritması sonuçları bu bölümde görsel olarak sunulmaktadır. 11. sırada yer alan sonuca göre diğer 10 öznitelik değerlendirilmektedir. Analiz sonuçları ayrıntılı olarak incelenerek veri kümesine göre yorumlar yapılmaktadır. Çizelge 2'de belirtildiği üzere sonuca ait 8 durum bulunmaktadır. Analiz sonuçlarında bu 8 durum renkli olarak ve rakamla belirtilerek de görülmektedir.



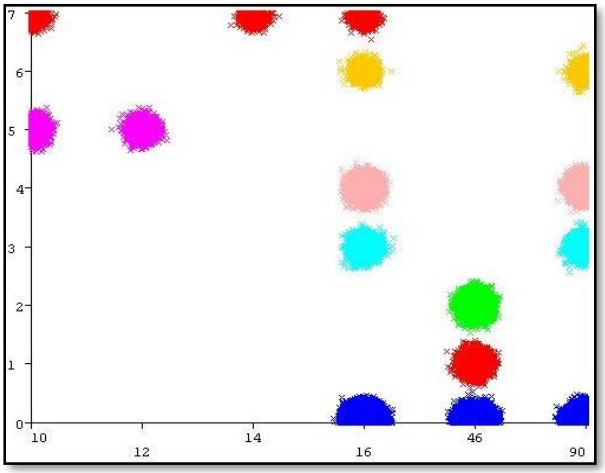
Şekil 3. Sonuç ile adres ilişkisi (Adresss relationship with result)

Şekil 3'te sonuç ile adres öznitelikleri arasındaki ilişkinin görseli yer almaktadır. Burada 7 farklı saldırı durumlarına (7,6,5,4,3,2,1 etiketlerine) ve normal duruma (0 etiketine) göre (toplam 8 durum), 20 adet adres değerinin değişimi görülmektedir. Buna göre sistemde 7. durum olan R atağı oluştuğunda, Modbus köle cihazının tüm istasyon adresleri ataktan etkilenmektedir. Diğer ataklarda ve normal durumda bir adet adres (4 etiketine sahip adres) etkilenmektedir.



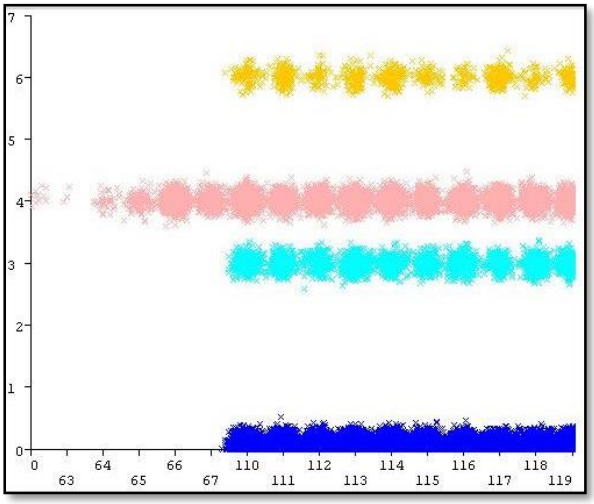
Şekil 4. Sonuç ile fonksiyon ilişkisi (Function relation with result)

Şekil 4'te sonuç ile fonksiyon öznitelikleri arasındaki ilişkinin görseli yer almaktadır. Burada 7 farklı saldırı durumlarına ve normal duruma göre 28 adet Modbus fonksiyon kodu değerinin değişimi görülmektedir. Buna göre sistemde 7. durum olan R atağı gerçekleştiğinde tüm kodlar ataktan etkilenmektedir. MFCI atağında ise 2 adet kod (8 ve 136 etiketlerine sahip kodlar) etkilenmektedir. MSCI, MPCI, DoS, NMRI ve CMRI atakları normal durum gibi davranmaktadır. Bu durumlarda 2 adet kod (3 ve 16 etiketlerine sahip kodlar) etkilenmektedir.



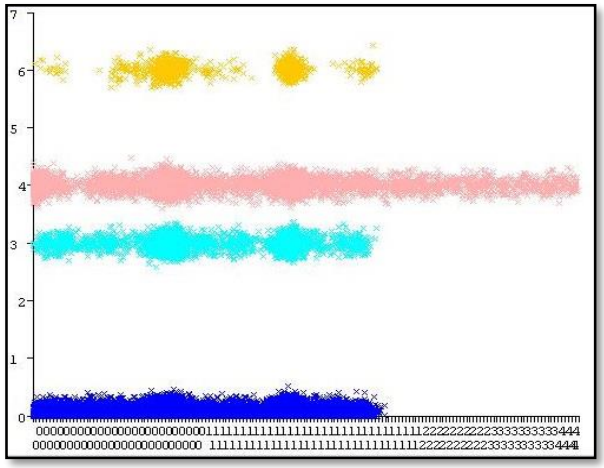
Şekil 5. Sonuç ile uzunluk ilişkisi (Length relationship with result)

Şekil 5'te sonuç ile uzunluk öznitelikleri arasındaki ilişkinin görseli yer almaktadır. Burada 7 farklı saldırı durumlarına ve normal duruma göre, 6 adet uzunluk değerinin değişimi görülmektedir. Buna göre sistemde 5 farklı atak türü görüldüğünde, Modbus paketinin büyüklüğü normal durumdaymış gibi davranmaktadır. Bunların dışındaki MFCI ve R atakları gerçekleştiğinde farklı paket büyüklükleri bu ataklardan etkilenmektedir.



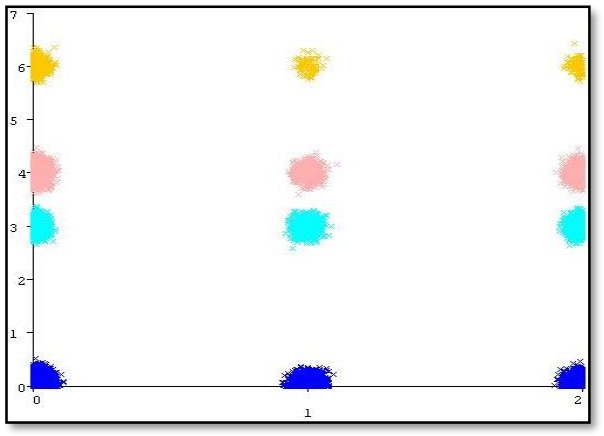
Şekil 6. Sonuç ile kazanç ilişkisi (Gain relationship with result)

Şekil 6'da sonuç ile kazanç öznitelikleri arasındaki ilişkinin görseli yer almaktadır. Burada 7 farklı saldırı durumlarına ve normal duruma göre 16 adet kazanç değerinin değişimi görülmektedir. Buna göre 4 farklı atak türünün de (R, MFCI, CMRI, NMRI) yaşandığı durumda PID kazancı görülmemektedir. PID, Mevcut sistem ile amaçlanan sitem durumları arasındaki farkın hesaplanmasını sağlamaktadır. Geri kalan 3 atak türü (DoS, MPCI, MSCI) yaşandığında meydana gelen PID kazancı normal durum ile yaklaşık olarak aynıdır. Bunların içinde yer alan MPCI atağı yaşanması durumunda elde edilen PID kazanç değer aralığı daha geniştir.



Şekil 7. Sonuç ile devir süresi ilişkisi (Cycle time relationship with result)

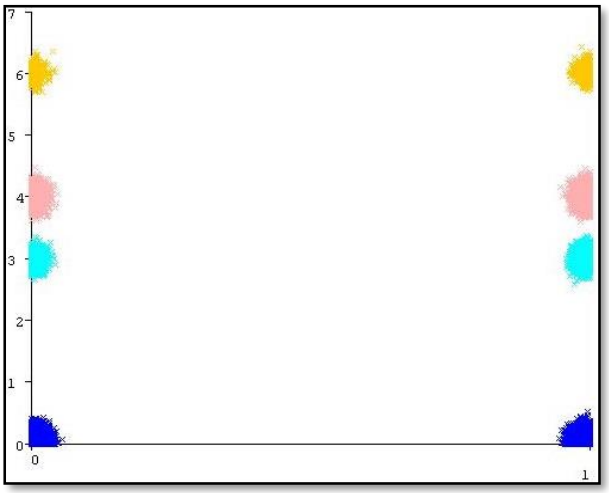
Şekil 7'de sonuç ile devir süresi öznitelikleri arasındaki ilişkinin görseli yer almaktadır. Burada 7 farklı saldırı durumlarına ve normal duruma göre 162 adet devir süresi değerinin değişimi görülmektedir. Buna göre 4 farklı atak türünün (R, MFCI, CMRI, NMRI) yaşanması durumunda PID devir süresi ile ilgili bilgi üretilmemektedir. Geri kalan 3 farklı atak türü (DoS, MPCI, MSCI) yaklaşık olarak normal durum ile aynı davranışa sahiptir. Bunların içinde yer alan MPCI atağı oluştuğunda PID devir süresi değer aralığı daha geniştir. Bu görsel üzerinden elde edilen sonuçlar, daha önce incelenen sonuç ile kazanç ilişkisine benzer sonuçlar içermektedir.



Şekil 8. Sonuç ile sistem şıkları ilişkisi (System mode relationship with result)

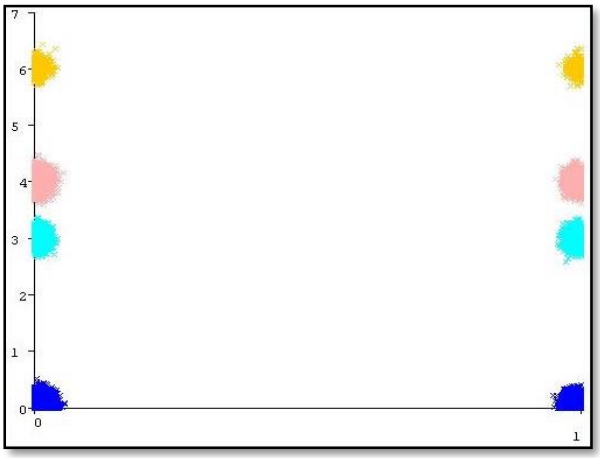
Şekil 8'de sonuç ile sistem şıkları öznitelikleri arasındaki ilişkinin görseli yer almaktadır. Burada 7 farklı saldırı

durumlarına ve normal duruma göre 3 adet sistem şıkkı değerinin değişimi görülmektedir. Buna göre 4 farklı atak türünün (R, MFCI, CMRI, NMRI) yaşanması durumlarında, sistem şıklarının hiçbiri görülmemektedir. Geri kalan 3 farklı atak türünde (DoS, MPCI, MSCI) ise sistem şıklarının değerleri normal durum ile aynı şekilde davranmaktadır.



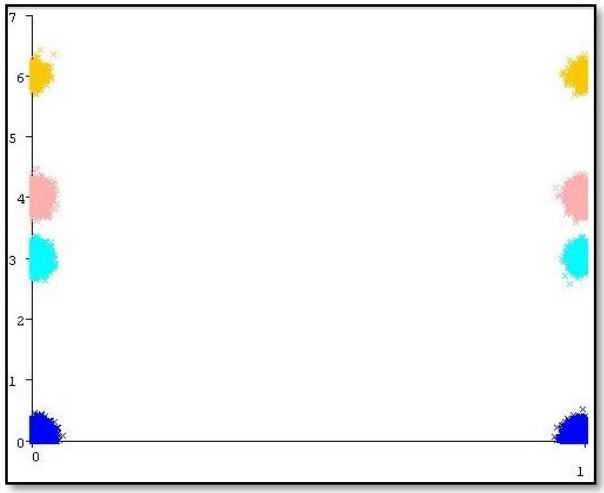
Şekil 9. Sonuç ile kontrol şeması ilişkisi (Control scheme relation with result)

Şekil 9'da sonuç ile kontrol şeması öznitelikleri arasındaki ilişkinin görseli yer almaktadır. Burada 7 farklı saldırı durumlarına ve normal duruma göre 2 adet kontrol şeması değerlerinin değişimi görülmektedir. Buna göre 3 farklı atak türü (DoS, MPCI, MSCI) yaklaşık olarak normal durum ile aynı davranışı sergilemektedir. Diğer 4 farklı atak türünün (R, MFCI, CMRI, NMRI) yaşanması durumunda ise kontrol şeması bilgisi sistemde görülmemektedir. Daha önce incelenen sonuç ile sistem şıkları ilişkisine benzer sonuçlar görülmektedir.



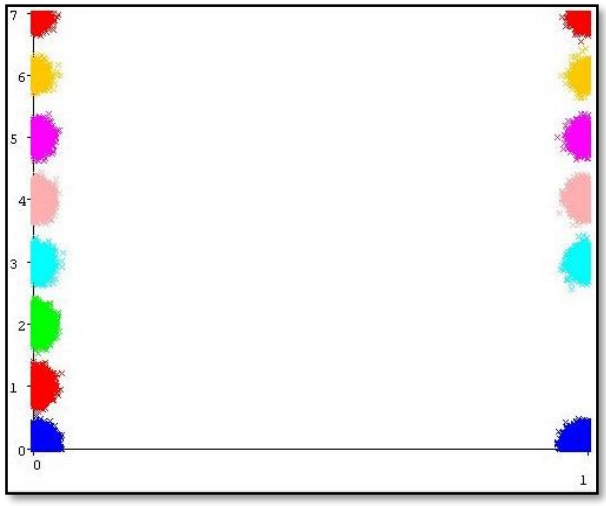
Şekil 10. Sonuç ile pompa ilişkisi (Pump relationship with result)

Şekil 10'da sonuç ile pompa öznitelikleri arasındaki ilişkinin görseli yer almaktadır. Burada 7 farklı saldırı durumlarına ve normal duruma göre 2 adet pompa değerlerinin değişimi görülmektedir. Buna göre 4 farklı atak türünün (R, MFCI, CMRI, NMRI) yaşanmasında da pompa kontrolü yapılmamaktadır. Geri kalan 3 farklı atak türünde (DoS, MPCI, MSCI) ise pompa kontrolü, normal durum ile aynı şekilde yapılmaktadır. Bu sonuçlar, daha önce incelenen sonuç ile sistem şıkları ilişkisine ve sonuç ile kontrol şeması ilişkisine benzer sonuçlar içermektedir.



Şekil 11. Sonuç ile solenoit ilişkisi (Solenoid relationship with result)

Şekil 11'de sonuç ile solenoit öznitelikleri arasındaki ilişkinin görseli yer almaktadır. Burada 7 farklı saldırı durumlarına ve normal duruma göre 2 adet solenoit değerinin değişimi görülmektedir. Buna göre 3 farklı atak türünün (DoS, MPCI, MSCI) yaşanması durumunda yapılan kontrol normal durum ile aynıdır. Geriye kalan 4 farklı atak türünün (R, MFCI, CMRI, NMRI) yaşanması durumunda ise tahliye vanası kontrolü yapılmamaktadır. Bu görsel dahil olmak üzere incelenen son dört ilişki görseli benzer sonuçlar sergilemektedir.



Şekil 12. Sonuç ile komut yanıtı ilişkisi (Command response relationship with result)

Şekil 12'de sonuç ile komut yanıtı öznitelikleri arasındaki ilişkinin görseli yer almaktadır. Burada 7 farklı saldırı durumlarına ve normal duruma göre 2 adet komut yanıtı değerinin değişimi görülmektedir. Buna göre cevap gönderilmesi seçeneği (0 numaralı etiket),

tüm atak türleri için normal durum gibi davranmaktadır. 2 farklı atak türü (CMRI, NMRI) yaşanması durumunda komut gönderilmesi seçeneği (1 numaralı etiket) görülmemektedir. Diğer atak türlerinde ise normal durum ile benzerlik görülmektedir.

5. DENEYSEL SONUÇLAR (EXPERIMENTAL RESULTS)

Bu çalışmada kritik altyapılardan gaz boru hattı kontrol sistemine yönelik gerçekleştirilen atakların yer aldığı veri kümesi analiz edilmiştir. Ayrıca SCADA veya EKS'lere yönelik meydana gelen siber terör atakları ele alınmıştır. Bu atakların davranışları ve normal durum ile farklılığı incelenmiştir. Bunun için çeşitli algoritmalar kullanılmış ve veri madenciliği yapılmıştır. Analiz sonuçlarına göre en yüksek doğru sınıflandırma oranına Random Tree algoritması sahip olmuştur. Bu algoritmanın çıktıları ayrıntılı şekilde incelenmiştir.

Veri kümesinde yer alan 6 farklı atak türü, 10 adet özniteliğe göre değerlendirilmiştir. Ayrıca, normal durum ile benzerlik gösteren davranışlar da incelenmiştir. Elde edilen deneysel sonuçlara bu bölümde yer verilmektedir.

7 numaralı Reconnaissance atağı gerçekleştiğinde:

- Modbus köle cihazının istasyon adreslerinin tümü ve Modbus fonksiyon kodlarının tümü etkilenmektedir.
- Farklı Modbus paket büyüklükleri etkilenmektedir.
- Komut-cevap gönderilmesi, normal (atak görülmeyen) durumla aynı davranışı göstermektedir.
- PID kazancı, PID devir süresi, sistem şıkkı, kontrol şeması, pompa ve solenoit öznitelikleri etkilenmemektedir.

6 numaralı Denial of Service atağı gerçekleştiğinde:

- 10 adet öznitelik için normal durumla aynı davranışlar gösterilmektedir.

5 numaralı Malicious Function Code Injection atağı gerçekleştiğinde:

- Modbus fonksiyon kodlarından 2 tanesi etkilenmektedir.
- Farklı Modbus paket büyüklükleri etkilenmektedir
- Modbus köle cihazının istasyon adresleri ve komut-cevap gönderilmesi, normal durumla aynı davranışı göstermektedir.
- PID kazancı, PID devir süresi, sistem şıkkı, kontrol şeması, pompa ve solenoit öznitelikleri etkilenmemektedir.

4 numaralı Malicious Parameter Command Injection atağı gerçekleştiğinde:

- PID Kazancı ve PID devir süresi değer aralıkları, normal duruma göre daha geniş şekilde etkilenmektedir.
- Diğer 8 adet öznitelik için normal durumla aynı davranışlar gösterilmektedir.

3 numaralı Malicious State Command Injection atağı gerçekleştiğinde:

- 10 adet öznitelik için normal durumla aynı davranışlar gösterilmektedir.

2 numaralı Complex Malicious Response Injection atağı gerçekleştiğinde:

- Modbus köle cihazının istasyon adresleri, Modbus fonksiyon kodları ve Modbus paket büyüklükleri normal durumla aynı davranışı göstermektedir.
- Komut-cevap gönderilmesinde ise cevap değeri normal durumla aynıyken komut durumu herhangi şekilde etkilenmemektedir.
- Diğer 6 öznitelik etkilenmemektedir.

1 numaralı Naive Malicious Response Injection atağı gerçekleştiğinde:

- Modbus köle cihazının istasyon adresleri, Modbus fonksiyon kodları ve Modbus paket büyüklükleri normal durumla aynı davranışı göstermektedir.
- Komut-cevap gönderilmesinde ise cevap değeri normal durumla aynıyken komut durumu herhangi şekilde etkilenmemektedir.
- Diğer 6 öznitelik etkilenmemektedir.

Elde edilen sonuçlara göre, Denial of Service ve Malicious State Command Injection atakları her öznitelik için normal durumla aynı şekilde davranmaktadır. Complex Malicious Response Injection ve Naive Malicious Response Injection atakları benzer şekilde hareket etmektedir. En fazla etkiyi Reconnaissance atağı gerçekleştirmektedir.

6. SONUÇ (RESULTS)

Bu çalışmada kullanılan veri kümesinde, mevcut SCADA protokollerinden Modbus için Command Injection, Reconnaissance ve Denial of Service gibi kategorilerde çeşitli ataklar gerçekleştirilmiştir. Bu veri kümesi kullanılarak SCADA veya EKS'lere yönelik atak yapılan ve atak yapılmayan durumlar farklı niteliklere göre değerlendirilip analiz edilmektedir. Bunun için Decision Stump, Hoeffding Tree, J48, Random Tree ve REP Tree algoritmaları veri madenciliği yapılarak kullanılmaktadır. En doğru sınıflandırma oranına Random Tree Algoritması sahip olduğu için bu algoritma sonuçları ayrıntılı olarak incelenmektedir. Siber terör ataklarının davranış analizleri ve atak tespiti üzerinde çalışılarak ilgili alana katkı sağlanması amaçlanmaktadır. SCADA atak tespiti sistemi araştırmalarında kullanılmak üzere yeni veri kümeleri sağlanmalıdır. Bunun için de bu tür saldırıların SCADA sistemlerine karşı uygulanması gereklidir. Bu konuda yapılacak çalışmalar SCADA güvenliğinin sağlanması için gereklidir.

Gelecekteki çalışmalar için farklı veri kümeleri elde edilerek siber terör atak davranış analizleri daha kapsamlı olarak gerçekleştirilecektir. Ayrıca elde edilen sonuçlar birbirlerine göre kıyaslanacak ve böylece çalışma alanı daha da genişletilecektir.

KAYNAKLAR (REFERENCES)

[1] TC Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, "Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, ulusal siber güvenlik stratejisi ve 2013-2014 eylem planı", **TC Ulaştırma, Denizcilik ve Haberleşme Bakanlığı**, Ankara, (2013).

[2] Igure V. M., Laughter S. A., Williams R. D., "Security issues in scada networks", **Computers & Security**, 25(7): 498-506, (2006).

[3] Morris, T., Thornton, Z., Turnipseed, I., "Industrial control system simulation and data logging for intrusion detection system research", **The 7th Annual Southeastern Cyber Security Summit,** Huntsvile, 1-6, (2015).

[4] Shang, W. L., Li, L., Wan, M., Zeng, P., "Security defense model of Modbus tcp communication based on zone/border rules", **International conference on network security and communication engineering,** Hong Kong, 1-8, (2014).

[5] Bhatia, S., Kush, N., Djamaludin, C., Akande, J., Foo, E., "Practical Modbus flooding attack and detection", **The Twelfth Australasian Information Security Conference**, New Zeland, 57–65, (2014).

[6] Hindy H., Brosset D., Bayne E., Seeam A., Bellekens X., "Improving SIEM for critical scada water infrastructures using machine learning", Computer Security, **Springer**, Cham, 2018.

[7] Hong, S., Lee, M., "Challenges and direction toward secure communication in the SCADA system", **The 8th Annual Communication Networks and Services Research Conference**, Montreal, 381-386, (2010).

[8] Kang, D., Lee, J., Kim, S., Park, J.,"Analysis on cyber threats to scada systems," **Transmission & Distribution Conference & Exposition: Asia and Pacific**, Seoul, 1-4, (2009).

[9] Dell, "Dell security annual threat report", **Dell**, Round Rock, (2015).

[10] Jung, S., Song, J. G., Kim, S., "Design on scada test-bed and security device", **International Journal of Multimedia and Ubiquitous Engineering,** 3(4): 75-86, (2008).

[11] Korkmaz E., Dolgikh A., Davis M., Skormin V., "Industrial control systems security testbed", **The 11th Annual Symposium on Information Assurance,** Albany, (2016).

[12] Hahn, A., Kregel, B., Govindarasu, M., Fitzpatrick, J., Adnan, R., Sridhar, S., Higdon, M. "Development of the powercyber scada security testbed", **The Sixth Annual Workshop on Cyber Security and Information Intelligence Research,** USA, (2010).

[13] Söğüt, E., Erdem, O. A., "A review of research studies on cyber terror", Applying Methods of Scientific Inquiry Into Intelligence, Security, and Counterterrorism, **IGI Global**, Hershey, 2019.

[14] Kurnaz, İ., "Siber güvenlik ve ilintili kavramsal çerçeve", **Cyberpolitik Journal**, 1: 62-83, (2017).

[15] Hekim, H., Başıbüyük, O., "Siber suçlar ve türkiye'nin siber güvenlik politikaları", **Uluslararası Güvenlik ve Terörizm Dergisi**, 4(2): 135-158, (2017).

[16] Yılmaz, S., "Türkiye'nin iç güvenlik yapılanmasında değişim ihtiyacı", **Çukurova Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**, 21(3): 17-40, (2012).

[17] Turnipseed, I., "A new scada dataset for intrusion detection system research", **Master's Thesis**, Mississippi State University, Electrical and Computer Engineering, (2015).

[18] Özbilen, A., "TCP/IP tabanlı dağıtık endüstriyel denetim sistemlerinde güvenlik ve çözüm önerileri", **Doctoral Thesis**, Gazi Üniversitesi, Fen Bilimleri Enstitüsü, (2012).

[19] TMMOB Elektrik Mühendisleri Odası, "Kontrol sistemleri-scada", **TMMOB Elektrik Mühendisleri Odasi Yayınları**, EK/2012/524, Ankara, (2012).

[20] Erkek, İ., "Modbus temelli scada sistemlerinin siber güvenliği için yeni bir yaklaşım", **Master's Thesis**, Gazi Üniversitesi, Fen Bilimleri Enstitüsü, (2012).

[21] Shahzad, A., Musa, S., Aborujilah, A., Irfan, M., "The scada review: system components, architecture, protocols and future security trends", **American Journal of Applied Sciences**, 11(8): 1418–1425, (2014).

[22] Mcdonald, J. D., "Developing and defining basic scada system concepts", **The 37th Rural Electric Power Conference,** Kansas City, 1-5, (1993).

[23] Kökver, Y., "Veri madenciliğinin nefroloji alanında uygulanması", **Master's Thesis**, Kırıkkale Üniversitesi, Fen Bilimleri Enstitüsü, (2012).

[24] Özarslan, S., "Öğrenci performansının veri madenciliği ile belirlenmesi", **Master's Thesis**, Kırıkkale Üniversitesi**,** Fen Bilimleri Enstitüsü, Kırıkkale, (2014).

[25] Witten, I. H., Frank, E., Hall, M. A., "Data mining: practical machine learning tools and techniques", **Morgan Kaufmann**, ISBN-10: 0128042915, Cambridge, (2016).