Avrupa Bilim ve Teknoloji Dergisi
Özel Sayı 30, S. 1-5, Aralık 2021

Araştırma Makalesi

www.ejosat.com ISSN:2148-2683

European Journal of Science and Technology
Special Issue 30, pp. 1-5, December 2021

Research Article

Yüksek Güvenlikli Ağlar İçin DDS Kullanılarak Tek Yönlü Güvenli Veri Aktarımı

Alper Kılıç[1*]

[1*] Konya Teknik Üniversitesi, Mühendislik ve Doğa Bilimleri Fakültesi, Bilgisayar Mühendisliği Bölümü, Konya, Türkiye, (ORCID: 0000-0002-1567-0213), akilic@ktun.edu.tr

(2nd International Conference on Computer, Electrical and Electronic Sciences ICCEES 2021, September 1-3, 2021)

(**DOI:** 10.31590/ejosat.993933)

ATIF/REFERENCE: Kılıç, A. (2021). Yüksek Güvenlikli Ağlar İçin DDS Kullanılarak Tek Yönlü Güvenli Veri Aktarımı. *Avrupa Bilim ve Teknoloji Dergisi*, (30), 1-5.

Öz

Bilgi güvenliğinin oldukça hassas olduğu kritik bilgiler içeren siber sistemlerin ve ağların yetkisiz erişim ve dış müdahalelerden korunması oldukça önemlidir. Ağ güvenliğinin sağlanması ve fiziksel olarak tek yönlü güvenli veri aktarımının yapılması için son yıllarda veri diyotları olarak isimlendirilen sistemler kullanılmaktadır. Tek yönlü veri aktarımı için veri merkezli bir ara katman mimarisi olan Data Distribution Service (DDS) gerek güvenli veri aktarımı özelliği gerekse barındırdığı yönlendirme, filtreleme ve izleme özellikleri ile oldukça uygun bir teknolojidir. Bu çalışmada DDS ara katman mimarisini kullanan tek yönlü güvenli veri aktarım sistemi önerilmiş ve performansı incelenmiştir. Buna göre kabul edilebilir performans kaybı olsa dahi kritik bilgiler içeren ağ sistemleri için DDS mimarisindeki tek yönlü iletim sisteminin uygun bir çözüm olabileceği, siber güvenlik sistemleri için birçok avantajı barındıran bir seçenek olacağı değerlendirilmiştir.

Anahtar Kelimeler: Ağ Güvenliği, Tek Yönlü Aktarım, DDS, Endüstriyel Ağlar, Veri Diyotları.

Unidirectional Secure Data Transfer Using DDS for High Security Networks

Abstract

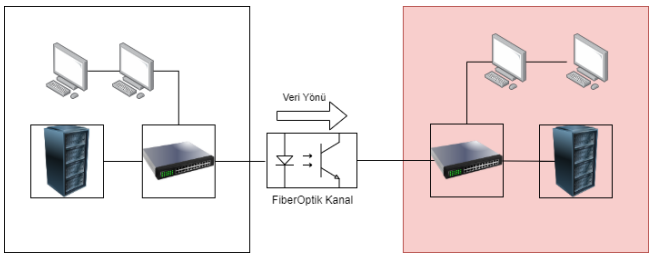
Protecting cyber systems and networks containing critical information, where information security is very sensitive, from unauthorized access and external interventions is very important. In recent years, systems called data diodes have been used to ensure network security and physically one-way secure data transfer. Data Distribution Service (DDS), which is a data-centric middleware architecture for one-way data transfer, is a very suitable technology with both its secure data transfer feature and its routing, filtering, and monitoring features. In this study, a one-way secure data transfer system using DDS middleware architecture is proposed and its performance is examined. Accordingly, it has been evaluated that one-way transmission system in DDS architecture can be a suitable solution for network systems containing critical information, even if there is acceptable performance loss, and it will be an option with many advantages for cyber security systems.

Keywords: Network Security, Unidirectional Data Transfer, DDS, Industrial Networks, Data Diodes.

[*] Sorumlu Yazar: akilic@ktun.edu.tr

1. Giriş

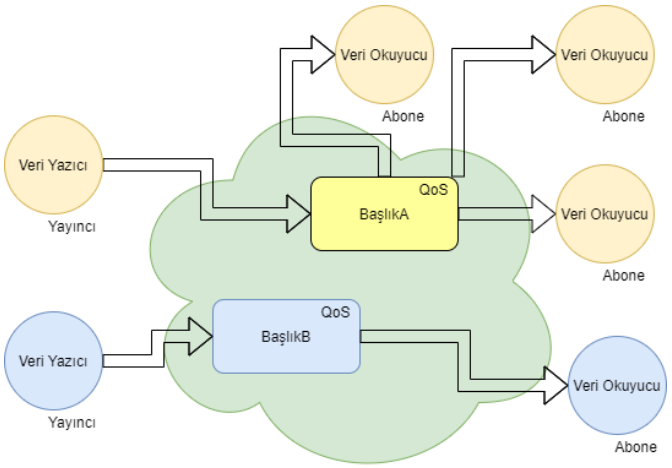
Hassas bilgiler içeren siber sistemlerin ve ağların yetkisiz erişim ve dış müdahalelerden korunması kritiktir. Endüstriyel kontrol ve izleme, proses kontrol ağları, kurumsal ağlar ve diğer ağ bağlantılı sistemlerin güvenliğini siber saldırı ve bilgi sızıntılarına karşı korumak için güvenlik duvarları (Anaya et al., 2009) veya akıllı anahtarlar gibi hem yazılım hem de donanım çözümleri içeren sistemler kullanılabilmektedir. Daha üst seviye koruma sağlamak ve gizlilik derecesine sahip bilgilerin fiziksel olarak da korunmasına yönelik olarak tek yönlü veri diyotları, fiziksel izoleli sözde/sanal hava boşluğu teknolojisi gibi farklı sistemler de kullanılmaktadır (Arkhangelskii et al., 2016; Rogowski, 2014; Van Besien et al., 2021). Tek yönlü aktarım için fiziksel bir engel oluşturan veri diyotları bilgi güvenliğini arttırarak farklı güvenlik seviyelerindeki ağlar arasında verinin tek yönde iletilmesini sağlayan araçlardır. Sadece gönderici→alıcı kanalı açık fiber optik bir aktarım ortamının kullanılması iki yönlü haberleşmeyi fiziksel olarak imkânsız hale getirmektedir (Şekil-1). Bununla birlikte TCP gibi donanım anlaşması (*handshaking*) kullanan ve ACK, NACK gibi sinyal cevaplarına ihtiyaç duyacak protokoller tek yönlü iletim sistemlerinde kullanılamayacaktır. Bu kapsamda literatürde donanımsal çözüm (Arkhangelskii et al., 2016), protokol dönüşümü (Reeves, 2015) ya da mesaj-dosya dönüşümü ve aktarımı yöntemi (Maatkamp et al., 2016) gibi farklı çözümlere rastlanmaktadır. Ticari ürünlerin de çoğu donanımsal çözümlere ek olarak kural tabanlı mesaj filtresi uygulaması ve protokol dönüşümünü entegre olarak kullanmaktadırlar (Menoher, 2013; Van Besien et al., 2021).



Şekil 1. Tek yönlü veri aktarım sistemi şeması

Ağ bileşenleri arasındaki veri alışverişi doğal olarak çift yönlü, asenkron ve yüksek performans gerektiren bağlantı modelini kullanmaktadır (Neelam & Shimray, 2021). Bununla birlikte siber saldırıların öncelikli amaçları sistemi işlevsiz hale getirmek, yetkisiz olarak veri toplamak ve tutarsız veri transferi ile bilgi güvenilirliğini azaltmak gibi (Yaşar & Çakır, 2015) hem saldırının hem de veri sızıntısının olduğu sistemler her defasında tehdit altında olacaktır. Bu kapsamda yönetim ve konfigürasyon kolaylığı gibi operasyonel faydalarından ötürü güvenlik duvarlarının yeteneklerinin arttırılması için çalışmalara rastlanabilmektedir (Anaya et al., 2009; Mukkamala & Rajendran, 2020). Bununla birlikte fiziksel olarak veri sızıntısının engellenmesine yönelik çalışmalar tamamen verinin tek yönlü aktarılması, güvenliğin arttırılması ve yüksek performansın sağlanmasına odaklanmıştır (Stevens, 1999).

Ağ bileşenlerinin güvenlik gereksinimlerini karşılamak üzere birçok hassas bilgiler içeren sistemlerin yetkisiz erişim ve dış müdahalelerden korunması, veri sızıntısının önlenmesi ve sistemin çalışır halde tutulması önemlidir. Bununla birlikte aktarılan verinin bütünlüğü, güvenilirliği ve aktarım başarısı da göz ardı edilmemelidir. Bu kapsamda son yıllarda veri merkezli aktarım ara katman mimarileri kullanılmaya başlanmıştır. Özellikle kritik sistemlerin veri paylaşımı için Data Distribution Service (DDS) (David et al., 2013; Pardo-Castellote, 2003) Object Management Group (OMG) tarafından önerilerek yayıncı-abone (*publish-subscribe*) metodolojisini merkeze alan ve birçok farklı servis kalitesi (QoS) sunan bir standart ara katman mimarisi sunmuştur. DDS ile uygulamalar veri transferi için gerekecek alt seviye kütüphaneler ile etkileşimden ziyade veri odaklı olarak belirli başlıklar(*topics*) kapsamında veri gönderimi yapabilir, ya da abone oldukları başlık altında yayınlanmış verilere taahhüt edilen servis kalitesi ile ulaşabilirler (Pardo-Castellote, 2003). Bu mimaride uygulamalar ağda serbest konumda bulunabilmekte, protokol, ağ adresi, port numarası, aktarım kimlik doğrulaması ya da yetkilendirilmesi gibi ağ konfigürasyonu ile ilgili konulardan soyutlanabilmektedir. Şekil-2'de ortak ağda bulunan bileşenler yerine veri merkezli olarak yayımcı rolündeki veri yazıcıları (*data writers*), abone rolündeki veri okuyucuları (*data readers*) ile başlık(*topic*) ve servis kaliteleri (*QoS*) şeması verilmiştir. Böylece ağ bileşenleri arasındaki iletişim çok daha net ölçeklenebilmekte, izlenebilmekte ve yönetilebilmektedir.



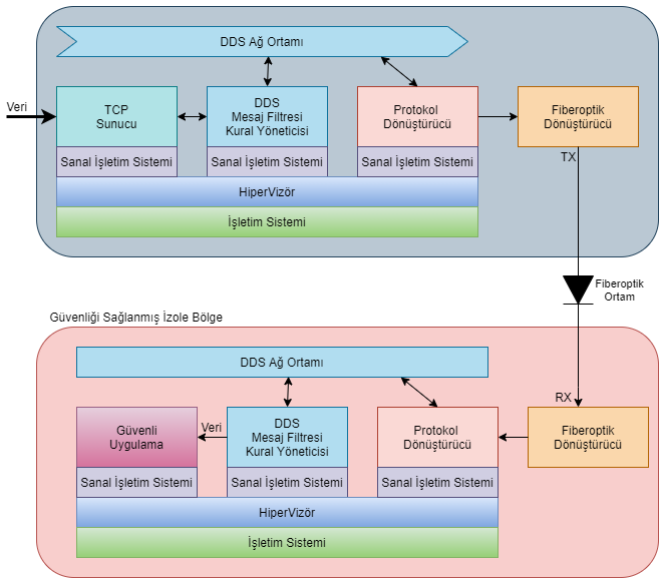
Şekil 2. DDS veri aktarım yaklaşımı şeması

DDS ara katman standardını gerçekleştiren yazılımlar (Baunthiyal, 2021; Kwon et al., 2017) yönlendirme, konfigürasyon, yönetim, izleme, kaydetme ve yeniden oluşturma benzeri birçok ek özellik de geliştirmişlerdir. Özellikle veri filtreleme, yönlendirme ve log özelliklerinin performansları oldukça dikkat çekicidir (Baunthiyal, 2021). Verinin semantik yapısına ve verinin kendisine odaklanan DDS tabanlı iletişim yazılımlarında standart iletişim katmanlarından öte filtre ve kurallar uygulanabilmektedir. Böylece TCP, UDP ya da RTPS (*Realtime Publish Subscribe*) gibi transport standartlarını kullanan fakat bağımlı olmayan veri merkezli bir yapı ortaya konabilmektedir. Verinin semantik olarak farklı başlıklar halinde gruplandığı ve iletildiği sistemlerde standart güvenliğin yanı sıra DDS ara katmanının güvenliğinin eklenmesi, güvenlik duvarı benzeri kural filtrelerinin eklenmesi ve bu ek özelliklerin performans etkisinin (Kang et al., 2020) en az olması oldukça önemli bir özelliktir.

Bu çalışmada "veri diyotu" olarak sınıflandırılabilecek DDS ara katman mimarisini kullanan tek yönlü güvenli veri aktarım sistemi önerilmiş ve performansı incelenmiştir.

2. Materyal ve Metot

Bu çalışmada tek yönlü güvenli veri aktarım sistemi için birbirlerinden fiziksel olarak izole edilmiş iki sistem bulunmaktadır (Şekil 3). Farklı sistemler kendi içlerinde sanallaştırılmış işletim sistemleri ile kısmen soyutlanarak ölçeklenebilirliği arttırılarak yönetim ve izleme kabiliyeti geliştirilmiştir. Aynı sistemdeki farklı sanal makineler üzerinde farklı görevler üstlenen yazılımlar geliştirilmiştir.



Şekil 3. Tek yönlü veri aktarım sistemi

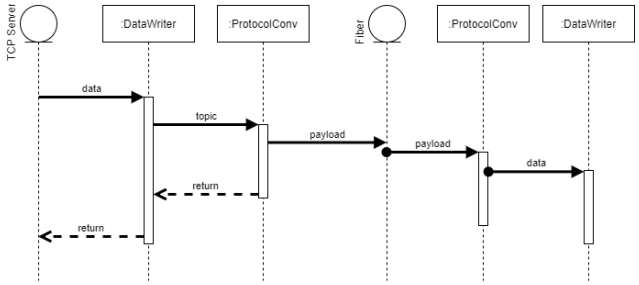
Şekil-3'te güvenli olmayan ön sistem (üstte) ve güvenliği sağlanmış izole sistem (altta) fiber optik ortam ile bağlanmıştır. Burada gönderici ve güvenli olmayan alanda sadece TX, alıcı ve güvenli tarafta da sadece RX kanalları arasındaki kablo bağlı olduğu için fiziksel olarak ters yönde akışın fiber optik kanaldan akışı mümkün olmayacaktır. Literatürde mikrofon ve hoparlör kullanılarak verinin akustik kanallardan aktarımının yapılabildiği, ya da elektromanyetik sızmaların da güvenlik tehdidi oluşturduğuna yönelik çalışmalar bulunsa da bu çalışmada kolaylıkla önlem alınabilecek bu tehditler sistemin genel yapısı açısından dikkate alınmamıştır. Ethernet fiber optik dönüştürücü için medya dönüştürücüler kullanılmıştır. DDS ara katman olarak eProsima fastDDS yazılım kütüphanesi kullanılmıştır. Performans ölçümü için kullanılan sistem ve yazılımlar Tablo-1'de verilmiştir.

Tablo 1. Sistem Konfigürasyonu

Sistem	Özellik
İşlemci	Intel I7-6500 CPU, 2.5GHz
RAM	16GB
Ağ	1000Mbps
Medya Dönüştürücü	TPLink MC210CS Gigabit, Single Mode
İşletim Sistemi	Ubuntu 18.04
Sanallaştırma	Virtual Box

Önerilen sistemde güvenli olmayan alan olarak belirlenmiş ön sistemdeki sunucu yazılımına gelen istekler sınıflandırılarak ayrıştırılır ve DDS veri yazıcısı ile sınıflandırılmış başlık altında yayınlanır. Farklı sanal makine üzerinde çalışan DDS yöneticisi aynı zamanda başlık yönlendiricisi ve veri filtresi olarak çalışmaktadır. Uygun başlıktaki veriler DDS ağ ortamı ile protokol dönüştürücü sanal makinesi üzerinde çalışan veri okuyucu tarafından uygun QoS ve kurallar çerçevesinde alınarak UDPv4 ya da ham Ethernet protokolüne dönüştürülür. Bu noktada her iki sistem arasında bulunan fiber kanalın kayıpsız olduğu varsayılmıştır. Yapılan çalışmalarda bit hata oranı 10^6 değerinden az olmasına rağmen hata düzeltme bitleri eklenmiş ve veri bütünlüğünün tamamlanması sağlanmıştır. Ayrıca ACK ve NACK sinyalleri göz ardı edilerek var olan protokollerin hata durumuna geçmesi engellenmiştir. Aşağıda TCP sunucusundan alınan veriye ait DDS IDL (*Interface Description Language*) yapısı ve veri geçiş diyagramı (Şekil 4) gösterilmiştir.

```
struct ServerIDL
{
    @Key long id;
    @Key string protocol;
    string sourceApplication;
    string info;
    Sequence<octet> payload;
    long payloadLength;
    unsigned short targetPort;
};
```



Şekil 4. Veri geçiş diyagramı

Performans ölçümü için düşük güvenlikli ağdan yüksek güvenlikli ağa dosya transfer uygulaması gerçekleştirilmiştir. Buna göre TCP sunucu için FTP (*File Transfer Protokol*) kullanılmıştır. FTP uygulamasında yüklenmek istenen dosya diske yazılmadan hafızada bölümler halinde tutulmuş, her bölüm FTP DDS başlığı altında protokol dönüştürücü yazılıma aktarılmıştır. Aynı şekilde dosya verileri octet dizisi (*sequence*) içerisinde kontrol edilerek aktarılarak ham Ethernet verisi şeklinde tek yönlü fiber optik kanala aktarılmıştır. Güvenliği sağlanmış izole fiber optik alıcı tarafta da dosya verisi içeren DDS paketleri toplanarak farklı sanal makinedeki uygulama yazılımına aktarılmış ve diske yazma işlemi tamamlanmıştır. Bu aşamada güvenli olmayan ağ tarafında hafıza bölgesine yazılan dosya bilgisi ile gönderici tarafın dosya transferinin tamamlandığı bilgisi aktarılmış fakat izole sisteme erişimi ve veri sızıntısı engellenmiştir.

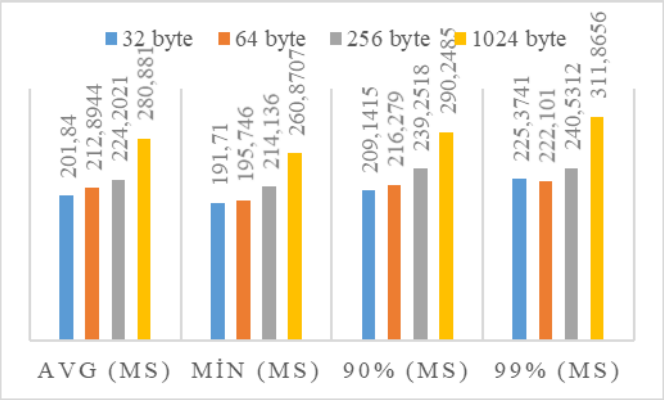
3. Araştırma Sonuçları ve Tartışma

Bu çalışmada DDS ara katman mimarisini kullanan tek yönlü güvenli veri aktarım sistemi önerilmiştir. Öncelikle güvenli olmayan alandan alınan veri semantik olarak ayrıştırılıp fiber optik kanal vasıtası ile güvenli tarafa aktarılmış ve aynı şekilde uygulama yazılımına iletilmiştir. Güvenli alanda olmayan sunucu tarafına veri ulaştıktan sonra güvenli alandaki uygulamaya kadar geçen süre ölçülmüş ve performansı

incelenmiştir (Tablo-2 ve Şekil-5). Örnek uygulamada FTP protokolü referans alınarak veriler 32-1024 byte arasında farklı segmentler şeklinde DDS başlıkları ile iletilmiştir. 10MB boyutundaki 250 adet dosya iletilmiş ve gecikme süreleri not edilmiştir. Gecikme miktarları veri boyutu artmasına rağmen oransal artmaması ile önerilen sistemin kabul edilebilir performansa sahip olduğu değerlendirilmiştir. Tablo-2'de gecikme miktarları sırasıyla ortalama, standart sapma, minimum ve maksimum olmak üzere bulunmaktadır. Bununla birlikte elde edilen ölçümlerin %90 ve %99 histogram değerleri tabloya eklenmiştir. Böylece maksimum gecikme miktarının %1 içerisinde olduğu anlaşılmıştır.

Tablo 2. Veri Gecikme Miktarı Tablosu

Veri (byte)	Ort (µs)	Std (µs)	Min (µs)	Maks (µs)	%90 (µs)	%99 (µs)
32	201,84	6,70	191,71	1327,29	209,14	225,37
64	212,89	8,07	195,74	2192,74	216,27	222,10
256	224,20	8,02	214,13	1895,81	239,25	240,53
1024	280,88	11,68	260,87	1820,56	290,25	311,87



Şekil 5. Sistem Performans Grafiği

4. Sonuç

Bilgi güvenliğinin hassas olduğu kritik sistemlerin ve ağların yetkisiz erişim ve dış müdahalelerden korunması oldukça önemlidir. Ağ güvenliğinin sağlanması ve fiziksel olarak tek yönlü güvenli veri aktarımının yapılması için son yıllarda veri diyotları olarak isimlendirilen sistemler kullanılmaktadır. Tek yönlü veri aktarımı için veri merkezli bir ara katman mimarisi olan Data Distribution Service (DDS) gerek güvenli veri aktarımı özelliği gerekse barındırdığı yönlendirme, filtreleme ve izleme özellikleri ile oldukça uygun bir teknolojidir. Bu çalışmada DDS ara katman mimarisini kullanan tek yönlü güvenli veri aktarım sistemi önerilmiş ve performansı incelenmiştir. Buna göre kabul edilebilir performans kaybı olsa dahi kritik bilgiler içeren ağ sistemleri için DDS mimarisindeki tek yönlü iletim sisteminin uygun bir çözüm olabileceği, siber güvenlik sistemleri için birçok avantajı barındıran bir seçenek olacağı değerlendirilmiştir.

DDS ara katman mimarisi yüksek performansa sahip, yönetilebilir ve ölçeklenebilir yapısıyla veri merkezli iletim uygulamaları için dikkate değer bir alternatiftir. Bu çalışmada belirtilen ve önerilen sistem farklı uygulamalar için uyarlanabilir. Gelecek çalışmalar için nesnelerin interneti kapsamında sürekli olarak belirli durumlarda veri iletecek ve güvenliği arttırılması gereken kritik sistemlerde (örn. nükleer santrallerin sensör verilerinin uzaktan izlenmesi) veri akışı güvenli taraftan güvenli olmayan tarafa şeklinde düzenlenerek kritik tesise herhangi bir veri sızıntısı engellenebilecektir.

Kaynakça

Anaya, E. A., Nakano-Miyatake, M., & Meana, H. M. P. (2009). A History and Survey of Network Firewalls. *Midwest Symposium on Circuits and Systems*.

Arkhangelskii, V., Epishkina, A., Kalmykov, V., & Kogos, K. (2016). Secure one-way data transfer. *Proceedings of the 2016 IEEE North West Russia Section Young Researchers in Electrical and Electronic Engineering Conference, EIConRusNW 2016*, 392–395. https://doi.org/10.1109/EIConRusNW.2016.7448203

Baunthiyal, A. (2021). Criteria Set for Evaluation of different DDS Distributions. *International Journal for Research in Applied Science and Engineering Technology*, *9*(1), 119–128. https://doi.org/10.22214/ijraset.2021.29243

David, L., Vasconcelos, R., Alves, L., André, R., & Endler, M. (2013). A DDS-based middleware for scalable tracking, communication and collaboration of mobile nodes. *Journal of Internet Services and Applications*. https://doi.org/10.1186/1869-0238-4-16

Kang, Z., Canady, R., Dubey, A., Gokhale, A., Shekhar, S., & Sedlacek, M. (2020). A study of publish/subscribe middleware under different iot traffic conditions. *M4IoT 2020 - Proceedings of the 2020 International Workshop on Middleware and Applications for the Internet of Things, Part of Middleware 2020 Conference*. https://doi.org/10.1145/3429881.3430109

Kwon, G., Park, J., Lee, G., Tak, T., Lee, W., & Hong, J. (2017). *Development of Real-Time Data Publish and Subscribe System Based on Fast RTPS for Image Data Transmission; Development of Real-Time Data Publish and Subscribe System Based on Fast RTPS for Image Data Transmission*. https://doi.org/10.18429/JACoW-ICALEPCS2017-TUPHA040

Maatkamp, M., van Delden, M., & LeKhac, N. A. (2016). *Unidirectional Secure Information Transfer via RabbitMQ*. *December*. https://doi.org/10.13140/RG.2.1.1412.0720

Menoher, J. (2013). All Data Diodes Are Not Equal. *Owl Computing*.

Mukkamala, P. P., & Rajendran, S. (2020). A Survey on the Different Firewall Technologies. *International Journal of Engineering Applied Sciences and Technology*. https://doi.org/10.33564/ijeast.2020.v05i01.059

Neelam, B. S., & Shimray, B. A. (2021). Observation of enhanced network performance in iot process control and data sensing with RINA. *Journal of Communications Software and Systems*. https://doi.org/10.24138/jcomss-2021-0027

Pardo-Castellote, G. (2003). OMG Data-Distribution Service: Architectural overview. *Proceedings - 23rd International Conference on Distributed Computing Systems Workshops, ICDCSW 2003*. https://doi.org/10.1109/ICDCSW.2003.1203555

Reeves, S. (2015). Tactical Data Diodes in Industrial Automation and Control Systems. *Whitepaper, SANS Institute*.

Rogowski, D. (2014). Software Support for Common Criteria Security Development Process on the Example of a Data Diode. *Proceedings of the Ninth International Conference*

DepCoS-RELCOMEX, *Advances in Intelligent Systems and Computing*, *286*, 363–372. https://doi.org/10.1007/978-3-319-07013-1

Stevens, M. W. (1999). *An Implementation of an Optical Data Diode*. 1–30.

Van Besien, W. L., Ferris, B., & Dudish, J. (2021). *Reliable, Efficient Large-File Delivery over Lossy, Unidirectional Links*. https://doi.org/10.1109/aero50100.2021.9438494

Yaşar, H., & Çakır, H. (2015). Kurumsal Siber Güvenliğe Yönelik Tehditler ve Önlemleri. *Düzce Üniversitesi Bilim ve Teknoloji Dergisi*.