Avrupa Bilim ve Teknoloji Dergisi
Özel Sayı, S. 530-536, Eylül 2020

Araştırma Makalesi

www.ejosat.com ISSN:2148-2683

European Journal of Science and Technology
Special Issue, pp. 530-536, September 2020

Research Article

Nesnelerin İnternetinde Sahte Kimlik Saldırılarının Makine Öğrenme Yöntemleri ile Tespiti

Semih Çakır[1*], Nesibe Yalçın[2] ve Sinan Toklu[3]

[1] Zonguldak Bülent Ecevit Üniversitesi, Kdz. Ereğli Meslek Yüksekokulu, Bilgisayar Teknolojileri Bölümü, Zonguldak, Türkiye (ORCID: 0000-0003-3072-9532)
[2] Bartın Üniversitesi, Mühendislik, Mimarlık ve Tasarım Fakültesi, Bilgisayar Mühendisliği Bölümü, Bartın, Türkiye (ORCID: 0000-0003-0324-9111)
[3] Düzce Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, Düzce, Türkiye (ORCID: 0000-0002-8147-9089)

(1st International Conference on Computer, Electrical and Electronic Sciences ICCEES 2020 – 8-10 October 2020)

(**DOI:** 10.31590/ejosat.838994)

ATIF/REFERENCE: Çakır, S., Yalçın, N. & Toklu, S. (2020). Nesnelerin İnternetinde Sahte Kimlik Saldırılarının Makine Öğrenme Yöntemleri ile Tespiti. *Avrupa Bilim ve Teknoloji Dergisi*, (Special Issue), 530-536.

Öz

Nesnelerin interneti (Internet of Things, IoT) cihazları, kablosuz algılayıcı ağlarında yaşanan gelişmelerle her geçen gün daha fazla kullanım oranına sahip olmaktadır. IoT cihazlarının tümünün birbirine bağlanması ile oluşan heterojen ağ, dışarıdan gelen saldırılara oldukça açıktır. Günümüze kadar birçok yönlendirme protokolü saldırıları ortaya atılmış olup gün geçtikçe saldırılar artmaya ve çeşitlenmeye devam etmektedir. Bununla birlikte, önerilen tespit ve önleme yöntemlerinin de günümüz şartlarına göre iyileştirilmesi ve güncel olması gerekmektedir. Sahte kimlik saldırıları, IoT' de ağ katmanında kayıplı ağlarda yönlendirme protokolünde (Routing Protocol for Low-Power and Lossy Network, RPL) yer almaktadır. Sahte kimlik saldırıları türünde düğümlerin sinyal gücüne bağlı saldırı tespitleri, en yaygın kullanılan ve önerilen yöntemlerdendir. Kaynak kısıtlı olan IoT cihazlarında, enerji korunumu ve düşük işlem yükü önemli hususların başında gelmektedir. Özellikle saldırı tespitinde kullanılan klasik yöntemler, saldırıların tespiti ve önlenmesinde yetersiz kalabilmektedir. Bu çalışmada, düğümlerin paket dağıtım oranları ve makine öğrenmesi yaklaşımlarından Naive-Bayes, Random Forest ve Lojistik Regresyon ile sahte kimlik saldırılarının tespiti önerilmiştir. Sahte kimlik saldırıları, klasik yöntemlere kıyasla daha yüksek başarım oranı (99.51% doğruluk) ile tespit edilmiştir.

Anahtar Kelimeler: Kablosuz Algılayıcı Ağlar, Nesnelerin İnterneti, RPL, Sahte Kimlik Saldırıları.

Detection of Sybil Attacks in IoT with Machine Learning Methods

Abstract

Internet of Things (IoT) devices are increasing their usage rates with advances in the wireless sensor networks. All IoT devices are connected to themselves with a heterogeneous network. Thus, they are also rather vulnerable to external attacks. Many routing protocol attacks have been described until now and continue to expand and diversify. Therefore, the recommended detection and prevention methods should be updated and improved according to today's condition. Sybil attack is a kind of the Routing Protocol for Low-Power and Lossy Network (RPL) attacks in IoT. The attack detection based on the signal strength of the nodes in Sybil attacks are one of the most commonly used and recommended approaches. In particular, classical methods that used to detect and prevent attack may not be appropriate for attack detection. The most critical problems in resource constrained IoT systems are energy consumption and heavy computational cost. In this study, packet distribution rates and machine learning approaches such as Naïve Bayes, Random Forest and Logistic Regression have been proposed for the prediction of Sybil attacks on RPL protocol in IoT networks. The Sybil attacks have been detected with 99.51% accuracy rate and this result is higher than classical methods for Sybil attack detection.

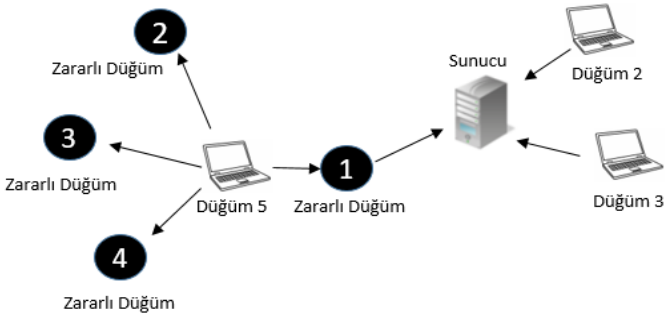
Keywords: Internet of Things, RPL, Sybil Attacks, Wireless Sensor Networks.

1. Giriş

İnternete erişimin daha kolay olduğu günümüzde teknolojik gelişmeler ile birlikte adından söz ettiren Nesnelerin İnterneti (Internet of Things, IoT), ilgi duyulan bir kavram olmaya devam etmektedir. Kısa menzil ve kablosuz bağlantı özelliği ile cihazlarda kullanıma sunulan bu teknoloji; giyilebilir cihazlarda, akıllı evlerde, e-sağlıkta, akıllı şehir alt ve üst yapılarında, akıllı endüstriyel uygulamalarda, lojistik, eğitim, turizm ve ticaret gibi birçok alanda dikkate değer uygulamaları ile karşımıza çıkmaktadır. IoT' de elektronik cihazlar, bünyesinde bulundurduğu algılayıcılar ile verileri alır ve analizini gerçekleştirebilir. Sunucu etrafında yer alan cihazlar insan etkileşimi olmadan birbirleri ile haberleşebilmektedir [1], [2]. Özellikle akıllı telefon teknolojisindeki gelişmelerin yanı sıra algılayıcıların cihazlara entegre edilmesi, mobil cihazlarla iletişimi kolay hale getirip farklı nesneleri IoT' nin bir parçası haline getirmektedir [3]. Her bir algılayıcı, sıcaklık, nem, ışık şiddeti gibi her türlü nicel özelliği diğer cihazlara ve kullanıcılara aktarabilmektedir. Ancak kaynak kısıtlı olması ve sınırlı işlem kapasiteleri, bu cihazları hassas hale getirmektedir [4].

Dünya üzerindeki son kullanıcıya yönelik saldırılar ve sistemleri aksatmaya neden olan kitlesel eylemler, IoT için de büyük tehdit oluşturmaktadır. En hassas yönü enerji olan bu nesneleri çeşitli saldırılarla etkisiz kılmak çok zor olmamaktadır. Ağ teknolojilerinde önemli çözüm teknolojileri sunan IEEE ve IETF, büyük bir yapıya ulaşacak IoT ortamının işlevsellik ve standardizasyon sorunlarına çözüm için öneriler sunmaktadır [5]-[7]. 2020 yılı itibariyle milyarlar ile ifade edilen düğüm sayısı için yetersiz kalacak olan IPv4 standardı yerine IoT ortamında IPv6 adresleri kullanılmaktadır. Enerji korunumu dikkate alındığında IETF tarafından Düşük Enerjili Kablosuz Kişisel Alan Ağları için IPv6 (IPv6 Over Low-Power Wireless Personal Area Networks, 6LoWPAN) bulunmuştur [6]-[8]. Veri bağlantı katmanı ile ağ katmanı arasında adaptasyonu sağlayan 6LoWPAN' ın bir parçası olan Düşük Enerjili ve Kayıplı Ağlar (Low-Power and Lossy Networks – LLNs) için Yönlendirme Protokolü (Routing Protocol for LLN, RPL) ile internet bağlantısı sağlanırken ağ katmanının daha verimli kullanılması için standartlaştırılmıştır [9].

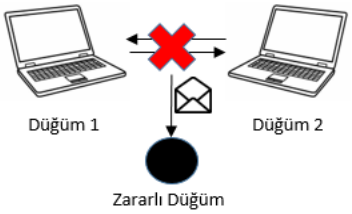
IoT' de yönlendirme protokolü RPL' de ve 6LoWPAN' da gerçekleşebilecek saldırı türlerinden biri olan Sahte Kimlik Saldırısı (Sybil Attack) bu çalışmada ele alınmıştır. Sahte Kimlik Saldırısı türünde zararlı düğüm, kendini komşu düğümlere birçok kimlik ile tanıtarak üzerine gelen paketleri onlara yönlendirir. Saldırıdan habersiz olan normal düğüm, kimlik değiştiren zararlı düğümden gelen paketi başka düğümden geliyormuş gibi algılar. Ağ içerisinde bu şekilde yönlendirilen paketler ağ trafiğini etkileyerek düğümlerin paket gönderip-almasını engelleyebilmektedir. Bir diğer etkide ise gerçek olan paket yerine sahte kimlikler tarafından oluşturulan paketler kök düğümde (sink node) toplanarak ağda iletilmesi gereken gerçek bilgi yerine sahte bilgiler ile ağın sürekliliğini ve kararlılığını bozabilmektedir [5]. Şekil 1' de 1 numara ile gösterilen düğüm sahte kimlik saldırısını yapan zararlı düğüm iken 2, 3 ve 4 numaralı düğümler ise zararlı düğümün sahte kimlikler ile oluşturduğu kopya düğümleri ifade etmektedir.



Şekil 1. Sahte Kimlik Saldırısını Gerçekleştiren Zararlı Düğümler

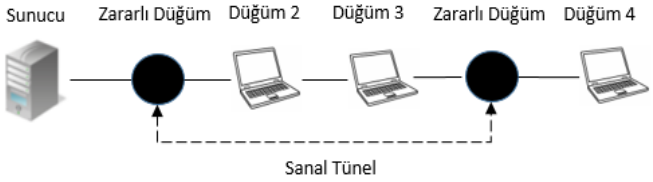
IoT' de yönlendirme protokolü RPL' de ve 6LoWPAN' da gerçekleşebilecek diğer saldırı türleri şu şekilde ifade edilebilir:

• Seçerek Yönlendirme Saldırısı: Normal düğüm gibi davranan zararlı düğüm, Şekil 2' de verildiği gibi ağ topolojisi içerisinde düğümler arası iletilen paketlerin iletilmesini engelleyebilir, gerektiğinde ağ ortamından paketleri düşürebilir. Bunun sonucunda düğümler arası gönderilen paketler ağ içerisinde yayılmamaktadır [10].



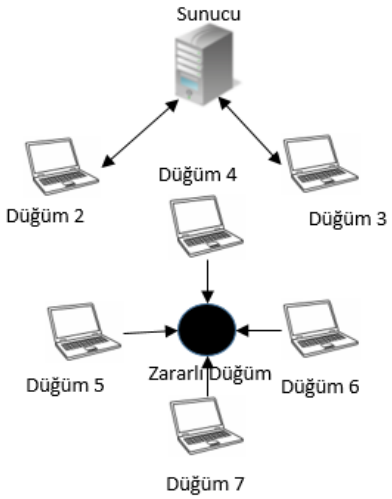
Şekil 2. RPL' de Seçerek Yönlendirme Saldırısı

• Solucan Deliği Saldırısı: Zararlı düğüm, ağda oluşturduğu iletim yönünden düşük hızda bir tünel yoluyla paketi bir noktadan diğerine iletir [11]. Şekil 3' te gösterildiği gibi zararlı düğümler sanal tünel oluşturarak paketin normal akışını değiştirmektedir.



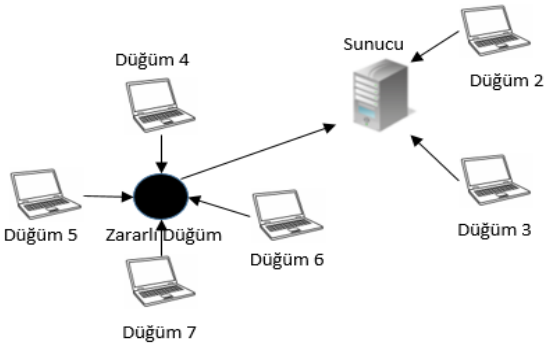
Şekil 3. RPL' de solucan deliği saldırısı

• Hello Taşkını: Servis aksatma saldırısının (DDOS) özellikleri görülmektedir. Bir algılayıcı ağda yönlendirme protokolü kendisinin var olduğunu komşu düğümlere belirtmek için kök düğüm gibi davranarak "Hello" mesajı yayınlar. Bu mesajı alan bir düğüm, kaynak düğümün iletişim mesafesi içinde olduğunu varsayarak bu kaynak düğümü komşuluk listesine ekleyebilir. Bunun sonucunda kaynakların tüketimi ile birlikte ağın işlevselliği yitirilebilir ve hizmetler aksayabilir [12]. Zararlı düğüm kendine komşu düğümlerin mesajlarını kendi üzerine yönlendirerek kök düğüm gibi davranmaktadır (bkz. Şekil 4).



Şekil 4. RPL' de Hello taşkını saldırısı

• Çukur Saldırısı: Zararlı düğüm, Şekil 5' te görüldüğü gibi ağ trafiğine etki etmek için paketleri belirli bir bölgeye ya da düşük maliyetli bir düğüm üzerine yönlendirerek bir çukur oluşturur [13]. Belirli düğümler üzerine yönlendirilen mesajlar kaynak kısıtlı olan düğümü işlevsiz kılabilmektedir.



Şekil 5. RPL' de çukur saldırısı

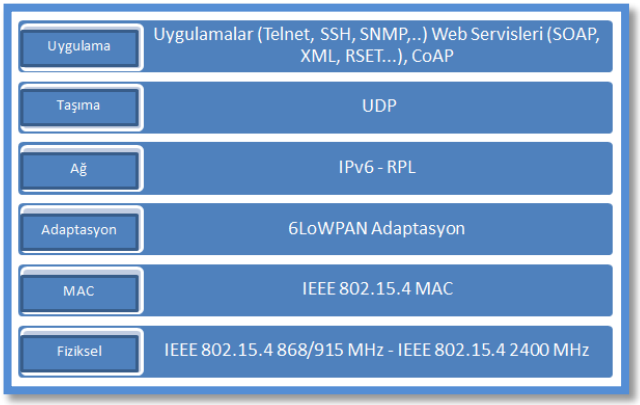
Ağa saldırı gerçekleştiren zararlı düğümün simülasyon ortamında gösterimini sağlayan birçok işletim sistemi ve simülasyon yazılımı bulunmaktadır. Contiki işletim sistemi Cooja simülatörü [14], IoT için kullanılan en son yazılımlardan olup içeriğine birçok farklı türde düğüm ekleme ve düğümler arası zamana bağlı haberleşmede paketlerin görüntülenmesini sağlayan yazılım türüdür. Simülasyon sonucu elde edilen veriler, Saldırı Tespit Sistemi (Intrusion Detection System, IDS) için yöntemler geliştirmeye yardımcı olmaktadır.

Bu çalışmada, Contiki-Cooja simülatörü kullanılarak düğümlerin paket dağıtım oranları ve makine öğrenmesi yaklaşımlarıyla sahte kimlik saldırılarının tespiti önerilmiştir. Sahte kimlik saldırıları, önerilen yöntem ile klasik yöntemlere kıyasla daha yüksek başarım oranı ile tespit edilmiştir.

2. Nesnelerin İnterneti (IoT) Teknolojileri ve RPL

2.1. IoT ve 6LoWPAN

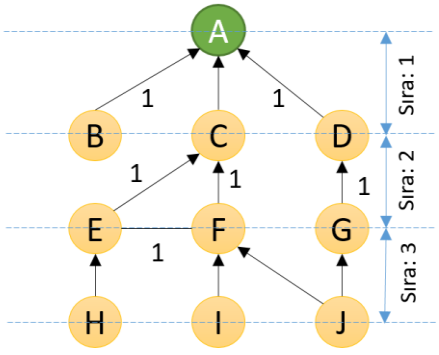
IoT, en yalın hali ile bir ağ topolojisi içerisinde heterojen nesnelerin birbirleri ile haberleşmesi olarak ifade edilebilir. IoT nesneleri (mobil cihazlar) elektronik temelli nesneler olduklarından kısıtlı seviyede işlemci, bellek ve çalışmaları için gerekli enerji kaynaklarına (batarya vb.) sahiptirler. Dış ortamda bulunan verileri alma, analiz etme, paylaşma ve depolama gibi özellikleri ile geniş kullanım alanlarında faaliyet göstermektedirler. Yakın gelecekte kullanım alanlarının artmasıyla sayıları 50 milyarı bulacak IoT cihazları için yetersiz kalacak olan IPv4 adresleri yerine IPv6 adresleri kullanılmaktadır. Bu sebeple, kaynak kısıtlı olan bu nesneler için düşük enerjili kablosuz kişisel alan ağlarında - 6LoWPAN [15], [17] IPv6 adreslerinin kullanılması zorunlu görülmektedir. Ortam erişim kontrolü (Media Access Control, MAC) ile ağ katmanı arasında yer alan bu adaptasyon katmanı Şekil 6' da verilmiştir. 6LoWPAN, çalışmanın da temeli olan RPL yönlendirme protokolü ile veri bağlantı katmanı arasında önemli bir yere sahiptir. En önemli özelliği ise IEEE 802.15.4 [16] standardına uygun olarak aynı anda birden fazla nesnenin haberleşmesini ve bunu da daha az işlem gücü, bellek kullanımı ve karmaşıklık hesabı ile gerçekleştirebilmesidir.



Şekil 6. 6LoWPAN Katman ve Protokol Yapısı [15]

2.2. RPL

RPL, kısıtlı enerjiye sahip ve hata seviyesi fazla olan ağlar için IPv6 yönlendirme protokolüdür [5] ve dinamik olarak kök düğüm ile normal düğümler arası yolları bulmak için yönlendirme protokolleri kullanarak ağın yapılandırılmasını sağlamaktadır. RPL, 6LoWPAN' da ki düğümler arasında hedefe yönelik yönlendirilmiş döngüsel olmayan bir grafik (Destination Oriented Directed Acyclic Graph, DODAG) oluşturur. Böylelikle 6LoWPAN cihazları arasında ve kök düğüm arasındaki veri trafiğinde meydana gelebilecek karmaşıklığı engeller. DODAG içerisinde yer alan düğümler kök dizinden aşağı yönlü bir ağaç düzenine benzer şekilde her düğüm belirli bir konuma ve sıraya sahiptir. Sıralar kök düğümden aşağı doğru artarken, aşağıdan kök düğüme doğru azalmaktadır. Şekil 7' de RPL' de DODAG yapısı gösterilmiştir. Burada A düğümü kök, B-J düğümleri ise DODAG yapısını oluşturan diğer düğümleri ifade etmektedir.

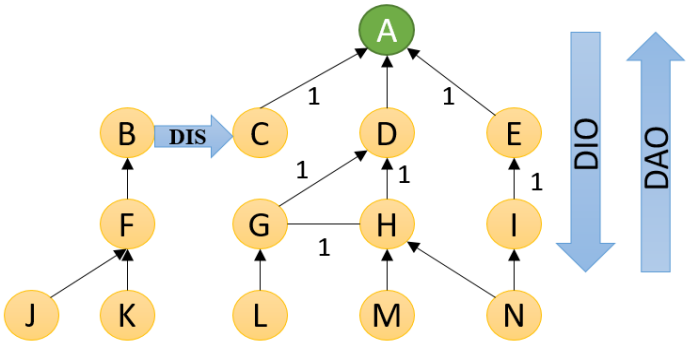


Şekil 7. RPL' de DODAG Yapısı

A düğümünden aşağı yönlü bir dizilim incelendiğinde B, C ve D düğümleri 1. sırada, E, F ve G düğümleri 2. sırada, son olarak H, I ve J düğümleri ise 3. sırada DODAG içerisinde yerini almıştır. Örnek olarak E düğümünü incelersek; C, F ve H düğümleri ile komşu durumundadır. C düğümü ise tercih edilen ebeveyn pozisyonundadır.

A kök düğümü başlangıç alındığında B, C ve D düğümlerinin konumları itibari ile seviyeleri (rank) 1, E, F ve G düğümlerinin seviyeleri 2, H, I ve J düğümlerinin seviyeleri ise 3 olarak ifade edilmektedir. G düğümü incelendiğinde D düğümü ebeveyn, E ve F

düğümleri ise kardeştir. RPL yönlendirme protokolü ağ topolojisinin varlığını sürdürebilmesi için birtakım mesajlar yayınlar. Şekil 8' de DODAG içerisinde yayınlanan mesajlar gösterilmiştir.



Şekil 8. DODAG içinde DIO, DAO ve DIS Mesajları

RPL protokolünde kullanılan ana kavramlar;

DIO (DODAG Bilgi Nesnesi (Information Object)): Bu mesaj kök düğüm tarafından ağa gönderilir. Yeni düğümleri keşfetmek, çeşitli konfigürasyonları iletmek ve ağ topolojisi içinde iletişim kurmak için kullanılır. Herhangi bir düğüm DIO mesajını alırsa, gelen düğümün bulunduğu sıra numarasını ve metrik değerlerini de dikkate alarak ebeveyn-çocuk ilişkisi belirlenir.

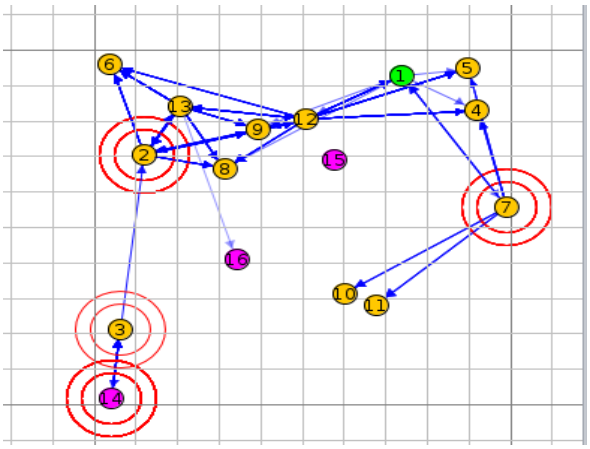
DIS (DODAG Bilgi İsteme (Information Solicitation)): DODAG ağına dâhil olmayan dışarıda yer alan bir düğüm DIS mesajı yayınlayarak ağa katılım isteği gönderir.

DAO (Destination Advertisement Object, Hedef İlan Nesnesi): Çocuk düğüm tarafından ebeveyne gönderilir. Bu mesaj, çocuğun DODAG yapısına katılım isteğine izin verme olarak ifade edilebilir. DAO-ACK ise kök veya ebeveynden gelen Evet ya da Hayır yanıtını içerir.

3. Uygulama

Literatürde klasik yöntemlere kıyasla makine öğrenme temelli algoritmalar ile daha başarılı sonuçlar elde edilmiştir. Çalışmada, kaynak kısıtlı olabilecek düğümlerin işlem yükü ve hafıza kapasiteleri de dikkate alınarak makine öğrenme yöntemleri ile sahte kimlik saldırısının tespiti amaçlanmıştır. Bu amaçla, çalışmada aşağıdaki adımlar gerçekleştirilmiştir:

a. Şekil 9' da gösterildiği gibi Sink mote tipinde 1 kök düğüm, 12 normal düğüm ve sahte kimlik saldırısı gerçekleştirecek 3 zararlı düğüm kullanılarak Contiki-Cooja simülasyon ortamında ağ kurulmuş ve 10 saat çalıştırılmıştır.



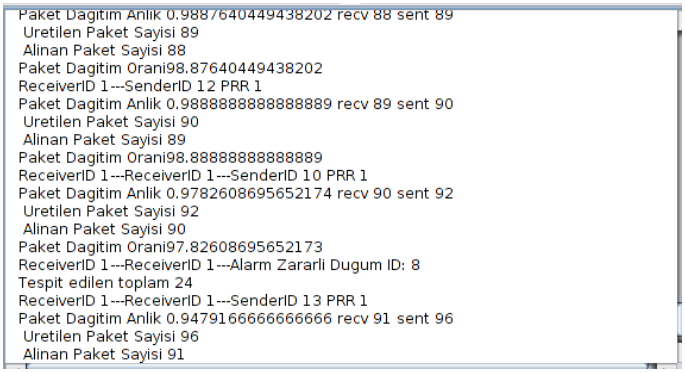
Şekil 9. Contiki-Cooja Simülatörü Ağ Topolojisi

b. Python yazılımı ile ".csv" uzantılı ham veriler, ".xlsx" formatına dönüştürülmüş ve düğümler arası paket gönderimi ve alımında kullanılan Tx (Radio Transmission) ve Rx (Radio Reception) özellikleri saldırı tespitinde kullanılmak üzere seçilmiştir.

c. Veri ön işleme ve özellik seçimi sonrası elde edilen veriler kullanılarak Naive-Bayes, Random Forest ve Lojistik Regresyon makine öğrenme algoritmaları ile sahte kimlik saldırısı tespiti yapılmıştır.

d. Paket Dağıtım Oranı (Packet Distribution Ratio, PDR) dikkate alınarak "izleme - monitoring" yöntemi ile kullanıcıya saldırı durumunda "alarm - alert" verilmiştir.

Contiki-Cooja Simülatörü Action Script Editor aracı ile elde edilen paket dağıtım oranı ve zararlı düğüm numarasını (mote ID) içeren görüntü kesiti Şekil 10' da verilmiştir.



Şekil 10. Sahte Kimlik Saldırısı ve Paket Dağıtım Oranı

Sahte kimlik saldırısı gerçekleştiren düğüm, ağa dâhil olduktan ve DODAG yapısı oluşturduktan sonra ağ trafiğini etkilemeye başlamaktadır. Ağda üretilen paket sayısı ile düğümler tarafından alınan paket sayısının birbirine oranı normal şartlarda 1' dir, 1' den küçük olması ağda paket kaybı olduğunu ve ağ topolojisinde bir saldırı durumunun söz konusu olduğunu ifade eder. Şekil 10' da anlık olarak verilen bazı veriler incelendiğinde zararlı düğüm ağı etkilemeye başladıktan sonra paket dağıtım oranında azalma meydana gelmiştir. İzleme yöntemi kullanılarak ağda saldırı gerçekleştiren düğüme ait kimlik bilgisi (mote ID) de ayrıca tespit edilmiştir.

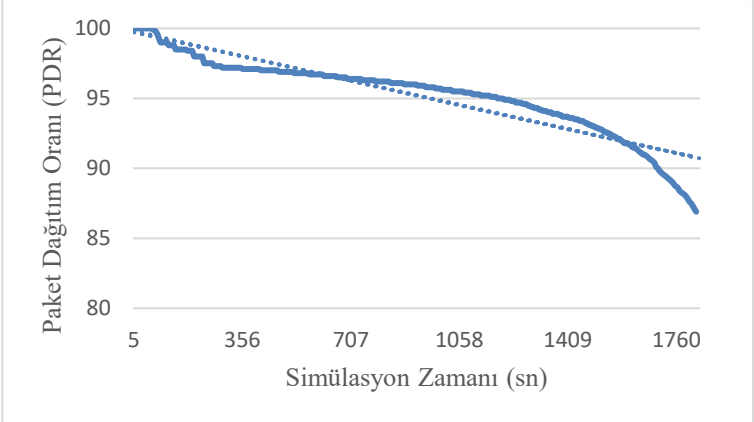
4. Sonuçlar

Makine öğrenme yöntemlerinden Naive-Bayes, Random Forest ve Lojistik Regresyon kullanılarak yapılan sahte kimlik saldırısı tespitinde elde edilen sonuçlar Tablo 1' de verilmiştir. En iyi başarımı %99,51 ile Naive Bayes algoritması, en kötü başarımı ise %96,12 ile Lojistik Regresyon algoritması göstermiştir.

Tablo 1. Makine Öğrenme Algoritmalarının Performans Karşılaştırması

Algoritma	**Doğruluk Oranı**
Naive-Bayes	% 99,10
Random Forest	% 99,51
Lojistik Regresyon	% 96,12

Düğümlerin konum ve paket dağıtım oranları, sahte kimlik saldırı tespitinde kullanılan diğer bir yöntemdir. İzleme yöntemi adı verilen bu tespit sisteminin, simülasyon başlangıcından itibaren ilk 1800 saniyelik veri analiz sonuçları Şekil 11' de verilmiştir. PDR azalış eğilimi gösteren grafikte en düşük değer %86,9 olarak elde edilmiştir.



Şekil 11. Saldırı Başlangıcı Sonrası PDR Değeri

5. Değerlendirme

Literatür incelendiğinde, sahte kimlik saldırı türü için saldırı tespit ve önleme yöntemi olarak rastgele anahtar dağıtımı, sinyal gücü, yer ve kod doğrulama yöntemleri kullanılmıştır. Bu yöntemler düğümler üzerindeki işlem yükünü arttırdığı gibi enerji tüketimlerini de etkilemektedir.

Dhamodharan vd. [18] çalışmalarında NS-2 simülatörü kullanarak kural tabanlı bir çözüm önermişlerdir. AODV protokolüne dayalı bir ağ oluşturulup mesaj kimlik doğrulaması ile sahte kimlik saldırısı tespiti gerçekleştirilmiştir. Sherasiya vd. [19] sahte kimlik saldırılarına karşı düğümlere ait sinyal uzunluğu hesabı (RSSI) ile belirledikleri sabit uzunluk değerini karşılaştırarak saldırı tespiti gerçekleştirmişlerdir. Dhanalakshmi vd. [20] çalışmalarında iki yöntem olan RAI - LVT tekniklerini NS-2 simülatöründe uygulayarak sahte kimlik atak tespitini %88 oranında başarı ile gerçekleştirmişlerdir.

Bu çalışmada, sahte kimlik saldırılarını tespit etmek için Naive-Bayes, Random Forest ve Lojistik Regresyon makine öğrenme yöntemleri kullanılmış ve en yüksek başarı oranı %99,51 ile Random Forest algoritması ile elde edilmiştir. Bu çalışmada yüksek doğrulukla tespiti gerçekleştirilen sahte kimlik saldırılarının önlenmesi bir sonraki çalışmada hedeflenmektedir.

Kaynakça

1. Tahsien, S. M., Karimipour, H., & Spachos, P. (2020). Machine learning based solutions for security of Internet of Things (IoT): A survey*, J. Netw. Comput. Appl.,* vol. 161.
2. Abane, A., Muhlethaler, P., Bouzefrane, S., & Battou, A. (2019). Modeling and Improving Named Data Networking over IEEE 802.15.4. *2019 8th International Conference on Performance Evaluation and Modeling in Wired and Wireless Networks (PEMWN)*, Paris, France, pp. 1-6, doi: 10.23919/PEMWN47208.2019.8986906.
3. Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. *Journal of Network and Computer Applications.*
4. Meghdadi, M., Özdemir, S., & Güler, İ. (2010). Kablosuz Algılayıcı Ağlarında Güvenlik: Sorunlar ve Çözümler. *Bilişim Teknol. Derg.*, vol. 1, no. 1, pp. 35–41.
5. Arış, A., Oktuğ, S., & Yalçın, S. B. Ö. (2015). Nesnelerin Interneti Güvenliği: Servis Engelleme Saldırıları. *23th Signal Processing and Communications Applications Conference (SIU)*, pp. 1–4.
6. Le, A., Loo, J., Lasebae, A., Vinel, A., Chen, Y., & Chai, M. (2013). The impact of rank attack on network topology of routing protocol for low-power and lossy networks. *IEEE Sens. J.*, vol. 13, no. 10, pp. 3685–3692.
7. Shelby, Z., & Bormann, C. (2011). 6LoWPAN: TheWireless Embedded Internet. vol. 43. New York, NY, USA: Wiley.
8. Hui, J., & Thubert, P. (2011). Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks. RFC 6282 (Proposed Standard), Internet Engineering Task Force.
9. Le, A., Loo, J., Lasebae, A., Vinel, A., Chen, Y., & Chai, M. (2013). The impact of rank attack on network topology of routing protocol for low-power and lossy networks. *IEEE Sensors Journal*, 13(10), 3685–3692. https://doi.org/10.1109/JSEN.2013.2266399.
10. Kaplantzis, S., Shilton, A., Mani, N., & Sekercioglu, Y. A. (2007). Detecting selective forwarding attacks in wireless sensor networks using support vector machines. *In Intelligent Sensors, Sensor Networks and Information, 3rd International Conference* on, pages 335–340.
11. Khan, F., Shon, T., Lee, T., & Kim, K. (2013). Wormhole attack prevention mechanism for RPL based LLN network. *Fifth International Conference on Ubiquitous and Future Networks (ICUFN)*, pp. 149–154.
12. Wallgren, S. R. L., & Voigt, T. (2013). Routing Attacks and Countermeasures in the RPL-Based Internet of Things. *International Journal of Distributed Sensor Networks*, vol. 2013, p. 11.
13. Weekly, K. & Pister, K. (2012). Evaluating sinkhole defense techniques in RPL networks. *20th IEEE International Conference on Network Protocols (ICNP)*, pp. 1–6.
14. Contiki, (2015). Contiki: The Open Source Operating System for the Internet of Things. http://www.contiki-os.org/, E.T. 19.01.2020.
15. Colina, A. L., Vives, A., Bagula, A., Zennaro, M., & Pietrosemoli, E. (2015). *IoT in 5 days.*
16. *IEEE Standard for Local and Metropolitan Area Networks – Part 15.4: Low Rate Wireless Personal Area Networks, (2011).* IEEE Std. 802.15.4-2011.
17. Demir, B., Ayrancıoğlu, G., Gezer, C., & Gözüaçık, N. (2016*). 6LoWPAN Kullanan Bir Algılayıcı Ağ Sistemi A Wireless Sensor Network System Using 6LoWPAN.* Elektrik-Elektronik ve Biyomedikal Mühendisliği Konferansı (ELECO 2016).
18. Dhamodharan, U. S. R. K., & Vayanaperumal, R. (2015). Detecting and preventing sybil attacks in wireless sensor networks using message authentication and passing method. *The Scientific World Journal,* 2015:7.
19. Sherasiya, T., & Upadhyay, H. (2016). Intrusion Detection System for Internet of Things. no. 3, pp. 2395–4396.
20. Dhanalakshmi, T. G., Bharathi, N., & Monisha, M. (2014). Safety concerns of Sybil attack in WSN. *International Conference on Science Engineering and Management Research, ICSEMR 2014*.