TWİTTERDA VERİ MADENCİLİĞİ YÖNTEMLERİN KULLANARAK BOT TESPİTİ

Alina AMANZHOLOVA

Gazi Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, alina.amanzholova@gazi.edu.tr

Doç. Dr. İbrahim Alper DOĞRU

Gazi Üniversitesi, Teknoloji Fakültesi, Bilgisayar Mühendisliği Bölümü, iadogru@gazi.edu.tr

Doç. Dr. Aysun COŞKUN

Gazi Üniversitesi, Teknoloji Fakültesi, Bilgisayar Mühendisliği Bölümü, aysunc@gazi.edu.tr

ÖZET

Twitter, günde 500 milyon tweet yayınlayan 319 milyon aylık aktif kullanıcıya sahip olan en popüler sosyal medya platformlarından biridir. Bu popülerlik Twitter'ı meşru kullanıcıları kimlik avı yapmak veya kötü amaçlı yazılımlar yaymak, tweet'lerde paylaşılan URL'leri kullanarak reklam vermek, meşru kullanıcıları takip etmek ve dikkatlerini çekmek, cinsel içerikli haberleri yaymak için trend olan konuları ele almak gibi nedenlerle Twitter'i kullanan spam göndericilerin dikkatini çekmektedir. Bu çalışmanın amacı, Twitter'da bot tespiti için kullanılan veri madenciliği yöntemlerinin en doğruluğu yüksek olanın belirtmektedir. Makalede, Twitter bot tespitinin özellikleri sunulmuştur. Ayrıca, literatürde sıkça kullanılan veri madenciliği yöntemleri: karar ağaçları, lojistik regresyon, Naive Bayes, Random forest sınıflandırma ve k Means kümeleme algoritmaların kullanarak Twitter'da bot tespiti yapılmaktadır. Hesap ve tweet üzerinden sınıflandırma doğruluğun yükseltmek için sınıflandırma algoritmaları ile SMOTE ve Resample teknikleri kullanmaktadır. Sonuç olarak kullanılan yöntemlerinin doğruluğu kategorize edilerek tartışılmıştır.

Anahtar Kelimeler: bot, Twitter, veri madenciliği, karar ağacı, sinir ağları, lojistik regresyon, random forest, Naive Bayes, k means, SMOTE, Resample

DETECTION OF BOTS USING DATA MINING METHODS IN TWITTER

ABSTRACT

Twitter is one of the most popular social media platforms with 319 million monthly active users that publish 500 million tweets per day. This popularity has caused Twitter to legitimate users, such as phishing or spreading malware, advertising using shared URLs in tweets, following legitimate users and attracting attention, and addressing trending topics to spread venereal content. The aim of this study is to identify the most accurate data mining methods used for bot detection on Twitter. In this article, features of Twitter bot detection are presented. In addition, data mining methods commonly used in the literature: decision trees, logistic regression, Naive Bayes, Random forest classification and k Means clustering algorithms are used to detect bot on Twitter. It uses SMOTE and Resample techniques with classification algorithms to improve the accuracy of classification through Account-based and tweet-based. As a result, the accuracy of the methods used was categorized and discussed.

Keywords: bot, Twitter, data mining, decision tree, neural networks, logistic regression, random forest, Naive Bayes, k means, SMOTE, Resample

1. GİRİŞ

Bot, robot'un kısaltılmış haliyle tanımlanan, bilgisayar veya yazılımlar üzerinde herhangi bir aktiviteyi yerine getirmekten sorumlu olan otomatik çalışan yazılımlardır. Botların aracılık ettiği çevrimiçi manipülasyon raporları politik konuşmayı [1], sahte haberleri [2], komplo teorilerini [3], borsa manipülasyonunu [4], insanların sağlığını [5], propaganda [6] ve bazı nadir durumlarda kullanılmıştır [7].

Botlar ayrıca siber güvenlik araştırma topluluğunun da ilgisini çekti: Bazen, büyük grup botlar, Twitter'da da gösterildiği gibi, siber saldırıları ve diğer siber güvenlik tehditlerini dağıtmak için kullanılan geleneksel botnet'lere benzer şekilde komuta-kontrol tarzında sahnelerin arkasında hareket eden, bot ustası olarak adlandırılan aynı varlık tarafından kontrol edilmektedir [8].

Bot tespitinde yapılan çok iş, sosyal medya verilerine kapsamlı erişim olduğunu varsaymaktadır. Örneğin, Wang ve ark. büyük ölçekli davranışsal anomalileri tanımlamak için kümeleme tekniklerini kullanmışlardır [9], diğer yazarlar ise bazı platformların tüm hesaplarını ve insanlardan ayrı botları analiz etmek için denetlenen öğrenmeyi kullandı [10]. Bazıları, örneğin SybilRank [11] veya Facebook Immune System [12] gibi uygulamaların etkinliğini gösteren çalışmalar yayınlanmıştır. Sınırsız veri erişiminin sınırlandırılmasını önlemek için, diğer teknikler daha küçük kullanıcı etkinliği örnekleri ve daha az etiketli bot ve insan kullanıcı örnekleri gerektirecek şekilde tasarlanmıştır. Böyle bir eğilimin örnekleri arasında, Chu ve arkadaşlarının [13] önerdiği sınıflandırma sistemi, Wang ve arkadaşlarının [9] tasarladığı kalabalığın kaynağına dayanan sistem, Clark ve arkadaşları [14] tarafından sunulan NLP'ye dayalı tespit teknikleri ve BotOrNot [15].

Şu anda Twitter'da 319 milyon aylık aktif kullanıcı olmaktadır. [16] University of Southern California ve Indiana University'den yapılan araştırmalara dayanarak bunların% 15'ine varan botlar. Bu, kabaca 48 milyon hesabın insanlar değil, botlar olduğu anlamına gelmektedir.

Bu makale akışı: Bölüm 2 literatür incelemesi, Bölüm 3'te Kullanılan veriseti, bot tespitinde yapılan deneysel sonuçlar ise 4 Bölümde ve son olarak 5 Bölümde sonuç ve öneriler verilmektedir.

2. LİTERATÜR İNCELEMESİ

Literatürde geçen Twitter'da bot algılama çalışmaları aşağıda verilmiştir.

Tablo 1. Literatürde Geçen Twitter'da Bot Tespit Etme Çalışmaları

Çalışma	Teknik	Metod	Veri seti
Deep neural networks for bot detection. Sneha Kudugunta, Emilio Ferrara (2018)	Derin sinir ağları	Hesap üzerinden: SMOTE Tweet üzerinden: LSTM	Cresci ve işbirlikçilerinin veri seti (2017) 8386 kullanıcı hesapları ve 11,834,866 tweetler
İdentifikatsiya botov v sotsialnyh setyah na baze tehnologiy intellektualnogo analiza dannyh. A.O. Evseeva, R.İ. Gumerova, A.S.	Veri madenciliği	Hesap üzerinden: 1. Sinir ağları 2. Karar ağacı 3. Lojistik regresyon Tweet üzerinden: -	200 kullanıcı hesabı içerisinde 50 kullanıcı bot

Katasev, A.P. Kirpiçnikov (2017)			
Empirical Evaluation and New Design for Fighting Evolving Twitter Spammers. C. Yang, R. Harkreader, G. Gu (2011)	Makine öğrenmesi	Hesap üzerinden: - Tweet üzerinden: 1. Google Güvenli Tarama (GSB) 2. URL honeypot	500.000 Twitter hesabı ve 14 milyondan fazla tweet içeren büyük bir veri
Detecting Automation of Twitter Accounts: Are You a Human, Bot, or Cyborg? Z.Chu, S. Gianvecchio, H. Wang, S. Member (2012)	Makine öğrenmesi	Hesap üzerinden: Depth-First Search (DFS) Tweet üzerinden: -	Twitter'dan toplam 512.407 kullanıcı veri seti
Online Human-Bot Interactions: Detection, Estimation, and Characterization. O.Varol, E. Ferrara, C.A. Davis, F. Menczer, A. Flammini	Makine öğrenmesi	Hesap üzewrinden: K-Means Tweet üzerinden: -	Twitter'dan toplam 14 miliyon kullanıcı veri seti
Measuring bot and human behavioral dynamics. I.Pozzana, E.Ferrara (2018)	Veri madenciliği	Hesap üzerinden: 1. Karar ağacı 2. Ekstra ağaçı 3. Random Forests 4. k En Yakın Komşular Tweet üzerinden: 1. Karar ağacı 2. Ekstra ağaçı 3. Random Forests 4. k En Yakın Komşular	380.000 heap 16 milyon tweet

Tablo 1'de görüldüğü gibi en çok kullanılan veri madenciliği yöntemlerinin kullanarak, bir sonraki bölümde bot tespiti yapılmaktadır.

SMOTE ve LSTM tekniklerin kullanarak, Kudugunta ve Ferrara çalışmasında dengesiz veri seti üzerinden bot tespiti yapılmıştır [17]. Hesap üzerinden SMOTE tekniğin kullanarak 99,81% ve tweet üzerinden LSTM tekniğin kullanarak 96,33% yüksek doğruluğu elde etmişlerdir. Diğer bir O.Varol ve arkadaşlarının çalışmasında 14 milyon kullanıcı üzerinden normal ve bot kullanıcıların tespit etmişlerdir. K- means algoritmasın kullanarak yüksek 94% doğruluğu elde etmişlerdir [18]. Aynı doğruluğu elde eden, I.Pozzana ve E.Ferrara çalışmasında karar ağacı, ekstra ağaç, random forest, k-means algoritmaların kullanarak bot tespiti yapılmıştır [19]. A.O. Evseeva ve arkadaşlarının çalışmasında ise veri madenciliği yöntemlerin kullanarak bot tespiti yapılmıştır. Karar ağacı, lojistik regresyon ve sinir ağları yöntemlerinin hata yüzdelerin karşılaştırıp, en iyi yöntem olarak sinir ağların belirtmişlerdir [20].

Bu çalışmada, liteatürde çok kullanılan veri madenciliği yöntemleri: karar ağacı, lojistik regresyon, Naive Bayes sınıflandırma ve k-means kümeleme algoritmaların kullanarak bot tespiti yapılmaktadır. Ayrıca, deneysel sonuçları daha da iyileştirmek için veri madenciliği yöntemleri ile birlikte hesap üzerinden SMOTE ve tweet üzerinden Resample tekniklerin kullanılmaktadır.

3. DATASET

Çalışmalarımızda kullanılan veri seti, Cresci ve işbirlikçilerinin [21] tamamen yeni bir bot verilerin içeren verisetidir. Tüm bu verilerden traditional_spambots1 klasöründen 998 bot kullanıcı hesabı ve genuine_accounts klasöründen 3472 normal kullanıcı hesabını, toplamda 4470 kullanıcı hesabın kullanacağız. Ayrıca, aynı sayıda traditional_spambots1 klasöründen 998 bot tweet hesabı ve genuine_accounts klasöründen 3472 normal tweet hesabını, toplamda 4470 tweet hesabın elde edilmektedir.

Birçok yerleşik teknik çok sayıda özellik kullanmasına rağmen ([15], örneğin 1500'ün üzerinde özellik kullanır), son zamanlarda yapılan araştırma [22,23], asgari sayıda özellik kullanılarak benzer yüksek performans elde edilebileceğini göstermektedir. Hesap düzeyinde bot tespiti için Tablo 2'de gösterilen aşağıdaki özellikleri kullanılmaktadır:

Tablo 2. Hesap Düzeyinde Bot Tespitinde Kullanılan Özellikler

Özellikler	Açıklama
Statuses Count	Hesabın toplam Durum Sayısı
Followers Count	Hesabın toplam Takip Sayısı
Friends Count	Hesabın toplam Arkadaşlar Sayısı
Favorites Count	Hesabın toplam Sık Kullanılanlar (favori) Sayısı
Listed Count	Hesabın toplam Listelenen Sayım
Default Profile	Hesabın Varsayılan Profili

Tweet düzeyinde bot tespiti için Tablo 3'te gösterilen aşağıdaki özellikleri kullanılmaktadır

Tablo 3. Tweet Düzeyinde Bot Tespitinde Kullanılan Özellikler

Özellikler	Açıklama
Retweet Count	Tweet'in toplam retweet sayısı
Reply Count	Tweet'in aldığı yanıt sayısı
Favorite Count	Tweet'in toplam favori sayısı
Number of Hashtags	Tweet'in toplam hashtag sayısı
Number of Mentions	Tweet'in toplam sayısı

3.1. Verileri Temizleme

Yöntemleri hesaplar ve tweetler üzerinde eğitmeden önce, her tweet'ten verileri önceden hazırlanmaktadır.

- Araştırmamıza gereksiz sütünleri silinmektedir.
- Hashtag'lerin, URL'lerin, sayıların ve kullanıcının sözlerinin oluşumunu "<hashtag>", "<url>", "<number>" veya '<user>" etiketleriyle değiştirilmektedir.
- Benzer şekilde, ortak emojiler belirli etiketlerle değiştirilmektedir. (ör. "<Smile>", "<heart>", "<lolface>", "<neutralface>" veya "<angryface>").
- Büyük harflerle yazılmış kelimeler veya tekrarlanan 2'den fazla harf içeren kelimeler için, kelimenin oluşumundan sonra yerleştirilen bir etiket. Örneğin, "HAPPY" kelimesi "happy" ve "<allcaps>" olmak üzere iki belirteçle değiştirilmektedir..
- Tüm belirteçler küçük harfe dönüştürülmektedir.
- Tüm tekrarlanan veriler alınmaktadır.

4. DENEYSEL SONUÇLAR

Önerilen yöntemde elde edilmiş etiketli veriler Karar ağaçları [24], Lojistik regresyon [25], Navie Bayes [26] sınıflandırma ve k-Means kümeleme algoritması [27] ile ayrı ayrı öğretilerek tespiti yapılmıştır. Bu işlem için Weka kullanılmıştır.

Elde edilmiş sonuçlar aşağıdaki Tablo 4'de verilmiştir.,

Tablo 4. Twitter'da Bot Tespiti Yöntemlerin Doğruluk Tablosu

Algoritma	Doğruluk (%)			
	Hesap üzerinden		Tweet üzerinden	
Karar ağacı	99,821	Normal-3 yanlış Bot-5yanlış	97,4938	Normal-89 yanlış Bot-23 yanlış
Lojistik regresyon	96,8897	Normal-40 yanlış Bot-99 yanlış	97,5386	Normal-87 yanlış Tweet-23 yanlış
Naive Bayes	96,0617	Normal-173 yanlış Bot-5 yanlış	96,7554	Normal-122 yanlış Tweet-23 yanlış
k Means	98,53	Normal - 30 Bot-7 yanlış	97,1134	Normal-106 yanlış Bot-23

Veri setimizi weka programının karar ağacı sınıflandırılmasın kullanarak uyguladığımızda hesap üzerinden 99.821, tweet üzerinden 97.4938 olan yüksek doğruluğu elde ettik. Karar ağacı algoritması hesap üzerinden sadece 3 kullanıcıyı yanlış bot olarak tespit etti. Aynı sayıda olan tweet üzerinden 89 tweetleri yanlış bot olarak tespit edilmiştir.

Diğer sınıflandırma algoritması lojistik regresyon kullanarak uyguladığımızda hesap üzerinden 99.8897, tweet üzerinden 97.5836 olan yüksek doğruluğu elde ettik. Lojistik regresyon sınıflandırma algoritması hesap üzerinden 99 bot kullanıcıları yanlış normal kullanıcı olarak, tweet üzerinden 23 bot tweetleri normal olarak yanlış tespit etti.

Sınıflandırma algoritmalarından son kullandığımız Naive Bayes sınıflandırılmasın kullandığımızda hesap üzerinden 96.0617, tweet üzerinden 96.7554 olan doğruluğu elde ettik. Naive Bayes algoritması hesap üzerinden 178 kullanıcıyı yanlış tespit etti ve aynı sayıda olan tweet üzerinden 155 tweetleri yanlış sınıflandırmıştır.

Sınıflandırma algoritmaları ile birlikte k means kümeleme algoritmasın kullanarak uyguladığımızda hesap üzerinden 98.53, tweet üzerinden 97.1134 olan yüksek doğruluğu elde ettik. K means kümeleme algoritması hesap üzerinden 37 kullanıcıyı yanlış tespit etti ve aynı sayıda olan tweet üzerinden 129 tweetleri yanlış sınıflandırmıştır.

4.1. Hesap Üzerinden SMOTE ile Sınıflandırma

Bölüm 3'te sunulduğu gibi, çok az veya hiç veri işleme gerektirmeyen az sayıda yorumlanabilir özellik kullanıyoruz. Bu, Bölüm 4'te sıralanan çok sayıda kullanıma hazır klasik veri madenciliği yaklaşımını kullanmamızı sağlar.

Çalışmamızda, bu yaklaşımların çoğunun % 90'ın üzerinde tatmin edici bir performansa sahip olduğunu bulduk. Bunlardan en başarılı olanı % 99.821 oranında bir doğruluk sağlayan Karar ağacına dayanıyor.

Bununla birlikte, veri setini aşırı örnekleme teknikleriyle, özellikle de sentetik azınlık aşırı örnekleme tekniği (SMOTE) ile dengeleyerek önemli performans kazanımları gözlemlenmiştir [28]. SMOTE algoritması, azınlık örneklerinin (örneğin, daha az sayıda etiketlenmiş veri noktasına sahip olan sınıf) özellik alanını temel alan örnekler oluşturur ve birçok alanda başarıyla görülen güçlü bir yöntemdir [29].

SMOTE yöntemin dengesiz hesap üzerinden veri setimize uyguladığımızda 1996 bot, 3471 normal kullanıcılar elde ederek sınıflandırılmıştır. Sonuçları aşağıdaki Tablo 5'te verilmektedir.

Tablo 5. Hesap Üzerinden Sınıflandırmasının Doğruluk Tablosu

Algoritma	Doğruluk (%)	
	Hesap üzerinden	
Karar ağacı + SMOTE	99,872	Normal-2 yanlış Bot-5 yanlış
Lojistik regresyon + SMOTE	99,2135	Normal-26 yanlış Bot-17 yanlış
Naive Bayes + SMOTE	96,8539	Normal-160 yanlış Bot-12 yanlış
k Means SMOTE	99,801	Normal- 6 Bot-3 yanlış

4.2. Tweet Üzerinden Resample İle Sınıflandırma

Resample, örnekleme oranını rasyonel bir faktörle değiştirmek için enterpolasyon ve desim birleştirmeyi ifade eder.

Örnekleme genellikle farklı örnekleme oranlarına sahip iki sistemi birbirine bağlamak için yapılır. İki sistemin ücretlerinin oranı bir tamsayıysa, örnekleme oranını değiştirmek için değerleme veya enterpolasyon kullanılabilir (oranın azalmasına veya artmasına bağlı olarak); Aksi takdirde, oranı değiştirmek için enterpolasyon ve azaltma birlikte kullanılmalıdır [30].

Resample yöntemin dengesiz tweet üzerinden veri setimize uyguladığımızda 1996 bot, 3471 normal kullanıcılar elde ederek sınıflandırılmıştır. Sonuçları aşağıdaki Tablo 6'da verilmektedir.

Tablo 6. Tweet Üzerinden Sınıflandırmasının Doğruluk Tablosu

Algoritma	Doğruluk (%)	
	Tweet üzerinden	
Karar ağacı + Resample	97,8742	Normal-134 yanlış Bot-56 yanlış
Lojistik regresyon + Resample	97,9526	Normal-87 yanlış Tweet-22 yanlış
Naive Bayes + Resample	97,382	Normal-178 yanlış Tweet-56 yanlış
k Means + Resample	99,98	Normal-1 Bot-1 yanlış

5. SONUÇ VE ÖNERİLER

Bu yazıda, Twitter'da bot tespitinin özellikleri ve literatürde önerilen yaklaşımlar göz önünde bulundurularak tartışılmıştır. Ayrıca, Twitter bot algılama yaklaşımları tarafından yaygın olarak kullanılan Twitter'ın eski özellikleri vurgulanmıştır. Twitter'ın, bildiğimiz kadarıyla, başka çalışmalardan da bahsetmediğimiz bazı yeni özellikleri de sunulmaktadır.

Bot tespitinde ekstra hiçbir yöntem kullanmadan Tablo 4'de görüldüğü üzere hesap üzerinden 99.821, tweet üzerinden 97.4938 başarı sağlayan karar ağacı sınıflandırma algoritmasını hesap üzerinden 98.53, tweet üzerinden 97.1134 olan k means kümeleme algoritması takip etmiştir. Veri setinin boyutunun arttırılması durumunda başarım oranlarında düşüş olabileceği öngörülmektedir. En düşük başarım oranı ise 4470 kullanıcılı veri setinde 3471 normal kullanıcıların 173 tanesini yanlış bot olarak ve 998 bot kullanıcıların 5 tanesini yanlış normal kullanıcı olarak, tweet üzerinden 4470 kullanıcılı veri setinde 3471 normal tweetlerden 122 tanesini yanlış bot olarak ve 998 bot kullanıcıların 23 tanesini yanlış normal kullanıcı olarak tespit eden Naive Bayes algoritması olmuştur.

Hesap üzerinden SMOTE yöntemin kullandığımızda karar ağacı sınıflandırmasında doğruluk 0.051 %, lojistik regresyon 2.2453 %, Naive Bayes 0.7922 %, k means 1.271 % doğruluk oranında artış görülmektedir. Bundan dolayı, bot tespitinde sınıflandırma yaparken, veri madenciliği yöntemleriyle birlikte SMOTE yönteminin kullanılması önerilmektedir.

Tweet üzerinden Resample yöntemin kullandığımızda karar ağacı sınıflandırmasında doğruluk 2.4862 %, lojistik regresyon 0.414 %, Naive Bayes 0.6266 %, k means 2.8666 % doğruluk oranında artış görülmektedir. Bundan dolayı, bot tespitinde tweet üzerinden sınıflandırma yaparken, veri madenciliği yöntemleriyle birlikte Resample yönteminin kullanılması önerilmektedir.

Bu çalışma, Twitter'da bot tespiti alanında araştırma yapan araştırmacılara yol göstereceği öngörülmektedir.

6. KAYNAKÇA

[1] A. Bessi , E. Ferrara. (2016). Social bots distort the 2016 us presidential election online discussion, First Monday 21 (11).

[2] A. Badawy, E. Ferrara, K. Lerman. (2018). Analyzing the digital traces of political manipulation: the 2016 Russian interference twitter campaign, arXiv: 1802. 04291.

[3] V. Subrahmanian , A. Azaria , S. Durst , V. Kagan , A. Galstyan , K. Lerman , L. Zhu , E. Ferrara , A. Flammini , F. Menczer. (2016). The darpa twitter bot challenge, Computer 49 (6), s 38–46 .

[4] E. Ferrara. (2015). Manipulation and abuse on social media, ACM SIGWEB Newslett. (Spring). 4.

[5] J. Allem , E. Ferrara. (2016). The importance of debiasing social media data to better understand e-cigarette-related attitudes and behaviors, J. Med. Internet Res. 18 (8).

[6] A. Badawy , E. Ferrara. (2018). The rise of jihadist propaganda on social networks, Journal of Computational Social Science. 1(2). s 453–470.

[7] B. Monsted , P. Sapiezynski, E. Ferrara , S. Lehmann. (2017). Evidence of complex contagion of information in social media: an experiment using twitter bots, PLoS ONE 12(9): e0184148. https://doi.org/10.1371/journal.pone.0184148 .

[8] N. Abokhodair , D. Yoo , D.W. McDonald. (2015). Dissecting a social botnet: growth, content and influence in twitter. Presented at the ACM conference on Computer-Supported Cooperative Work and Social Computing. s 839–851 .

[9] G. Wang , M. Mohanlal , C. Wilson , X. Wang , M. Metzger , H. Zheng , B.Y. Zhao. (2013). Social turing tests: crowdsourcing sybil detection, in: Proc. of the 20th Network & Distributed System Security Symposium (NDSS).

[10] I. Pozzana, E. Ferrara. (2018). Measuring bot and human behavioral Dynamics. arXiv: 1802.04286.

[11] Q. Cao , M. Sirivianos , X. Yang , T. Pregueiro. (2012). Aiding the detection of fake accounts in large scale social online services, in: 9th USENIX Symp on Netw Sys Design & Implement. s 197–210.

[12] T. Stein , E. Chen , K. Mangla. (2011). Facebook immune system, in: Proc. of the 4th Workshop on Social Network Systems, ACM. s 8 .

[13] Z. Chu, S. Gianvecchio, H. Wang, S. Jajodia. (2012). Detecting automation of twitter accounts: are you a human, bot, or cyborg? IEEE Trans. Depend. Secure Comput. 9 (6), s. 811–824.

[14] E. Clark, J. Williams, C. Jones, R. Galbraith, C. Danforth, P. Dodds. (2016). Sifting robotic from organic text: a natural language approach for detecting automation on twitter. J. Comput. Sci. 16 s. 1–7.

[15] C.A. Davis, O. Varol, E. Ferrara, A. Flammini, F. Menczer. (2016). Botornot: a system to evaluate social bots, in: Proceedings of the 25th International Conference Companion on World Wide Web, International World Wide Web Conferences Steering Committee, s. 273–274 .

[16] M. Newberg, CNBC 20.03.2017. [Online]. http://www.cnbc.com/2017/03/10/nearly-48-million-twitteraccounts-could-be-bots-says-study.html. [Erişim tarihi: 20.11.2018].

[17] S. Kudugunta ve E. Ferrara. (2018) Deep neural networks for bot detection. Information Sciences, 467, s. 312-322.

[18] O.Varol, E. Ferrara, C.A. Davis, F. Menczer ve A. Flammini. Online Human-Bot Interactions: Detection, Estimation, and Characterization. arXiv:1703.03107

[19] I. Pozzana, E. Ferrara. (2018). Measuring bot and human behavioral Dynamics. arXiv: 1802.04286.

[20] A.O. Evseeva, R.İ. Gumerova, A.S. Katasev, A.P. Kirpiçnikov. (2017). İdentifikatsiya botov v sotsialnyh setyah na baze tehnologiy intellektualnogo analiza dannyh. Vestnik tehnologicheskogo universiteta, 20(5), s. 87-90.

[21] S. Cresci , R. Di Pietro , M. Petrocchi , A. Spognardi , M. Tesconi. (2017). The paradigm-shift of social spambots: evidence, theories, and tools for the arms race, in: Proceedings of the 26th International Conference on World Wide Web Companion, International World Wide Web Conferences Steering Committee,s. 963–972 .

[22] E. Ferrara. (2017). Disinformation and social bot operations in the run up to the 2017 french presidential election, First Monday 22 (8).

[23] E. Ferrara , O. Varol , C. Davis , F. Menczer , A. Flammini. (2016). The rise of social bots, Commun ACM 59 (7) 96–104 .

[24] D.P. Zegjda, T.V. Stepanova. (2012). Ocenka effektivnosti ispolzovaniya sredstv zashity dlya neitralizaciy i ustraneniya bot-setei, Problemy informacionnoi bezopasnosti Komputerniye sistemy. 2. s 21-27.

[25] A.S. Katasev. (2013). Formirovaniye bazy znaniy sistemy filtraciy elektronnyh pochtovyh soobsheniy, Nauchno- tehnicheskiy vestnik Povoljya. 5. s. 191-194.

[26] Pawlak, Zdzisław. "A Rough Set View on Bayes' Theorem" (PDF) (İngilizce). (Erişim tarihi: 3 Ocak 2019)

[27] https://tr.wikipedia.org/wiki/K-means_kümeleme (Erişim tarihi: 6 Ocak 2019)

[28] N.V. Chawla, K.W. Bowyer, L.O. Hall, W.P. Kegelmeyer. (2002). Smote: synthetic minority over-sampling technique, J. Artif. Intell. Res. 16, s. 321–357.

[29] H. He, E.A. Garcia, Learning from imbalanced data. (2009). IEEE Trans. Knowl. Data Eng, 21 (9), s.1263–1284.

[30] https://dspguru.com/dsp/faqs/multirate/resampling/ (Erişim tarihi: 17 Ocak 2019)