Avrupa Bilim ve Teknoloji Dergisi
Özel Sayı 28, S. 1317-1320, Kasım 2021
© Telif hakkı EJOSAT'a aittir
Araştırma Makalesi

www.ejosat.com ISSN:2148-2683

European Journal of Science and Technology
Special Issue 28, pp. 1317-1320, November 2021
Copyright © 2021 EJOSAT
Research Article

Detection of DIS Flooding Attacks in IoT Networks Using Machine Learning Methods

Semih Çakır[1], Nesibe Yalçın[2*]

[1] Zonguldak Bülent Ecevit University, Departmant of Computer Sciences, Zonguldak, Turkey, (ORCID: 0000-0003-3072-9532), semih.cakir@beun.edu.tr
[2*] Erciyes University, Faculty of Engineering, Departmant of Computer Engineering, Kayseri, Turkey, (ORCID: 0000-0003-0324-9111), nesibeyalcin@erciyes.edu.tr

(1st International Conference on Applied Engineering and Natural Sciences ICAENS 2021, November 1-3, 2021)

(**DOI:** 10.31590/ejosat.1014917)

ATIF/REFERENCE: Cakir, S. & Yalcin, N. (2021). Detection of DIS Flooding Attacks in IoT Networks Using Machine Learning Methods. *European Journal of Science and Technology*, (28), 1317-1320.

Abstract

In today, Internet of Things (IoT) has a wide usage area and makes easier our lives with smart objects that can communicate with each other without human intervention. However, as with Wireless Sensor Networks, IoT networks bring new risks. These risks reaching worrying levels cause some significant issues such as security, privacy, and energy in the network topology. The IPv6 Routing Protocol for Low-Power and Lossy Network (RPL) is a routing protocol for resource-constrained devices in IoT networks. When it transmits packets between nodes, the nodes can be exposed to a series of attacks. DODAG Information Solicitation (DIS) Flooding attack is one of the most effective types of attacks against this protocol and negatively affects the energy level of the node and its limited processing capacities. Although many intrusion detection methods are used to detect attacks in IoT security, innovative and energy-saving methods are needed. DIS Flooding attacks detection and prevention methods have not been adequately presented in the literature. To address the mentioned need, this study provides high-performance detection of DIS Flooding attacks by applying Logical Regression (LR) and Support Vector Machine machine learning methods. The experiments are implemented by using the Contiki-Cooja simulation environment and the experimental results have been evaluated using various performance metrics. It can be concluded that LR achieves higher attack detection in terms of accuracy.

Keywords: Attack Detection, DIS Flooding, Internet of Things, Machine Learning, RPL.

Makine Öğrenmesi Yöntemleri Kullanılarak Nesnelerin İnterneti Ağlarında DIS Flooding Saldırılarının Tespiti

Öz

Günümüzde Nesnelerin İnterneti (Internet of Things, IoT) geniş bir kullanım alanına sahip olup insan müdahalesi olmaksızın birbirleriyle haberleşebilen akıllı nesnelerle hayatımızı kolaylaştırmaktadır. Ancak Kablosuz Algılayıcı Ağlar'da olduğu gibi, IoT ağları da yeni riskleri beraberinde getirmektedir. Endişe verici boyutlara ulaşan bu riskler, ağ topolojisinde güvenlik, gizlilik ve enerji gibi bazı önemli sorunlara neden olmaktadır. Düşük Güç ve Kayıplı Ağlar için IPv6 Yönlendirme Protokolü (RPL), IoT ağlarındaki kaynak kısıtlı cihazlar için bir yönlendirme protokolüdür. Düğümler arasında iletilen paketler bir dizi saldırıya maruz kalabilir. DODAG Information Solicitation (DIS) Flooding saldırısı, bu protokole karşı en etkili saldırı türlerinden biridir ve ağ içerisinde yer alan düğümlerin enerji seviyesini ve işlem kapasitelerini olumsuz etkiler. IoT güvenliğinde saldırıları tespit etmek için birçok saldırı tespit yöntemi kullanılsa da yenilikçi ve enerji korunumlu yöntemlere ihtiyaç duyulmaktadır. DIS Flooding saldırılarını tespit etme ve önleme yöntemleri literatürde yeterince ele alınmamıştır. Söz konusu eksikliği gidermek için bu çalışmada, Lojistik Regresyon (LR) ve Destek Vektör Makinesi yöntemleri kullanılarak DIS Flooding saldırılarının yüksek doğruluk oranı ile tespiti gerçekleştirilmiştir. Çalışmada Contiki-Cooja simülasyon ortamı kullanılmış ve deneysel sonuçlar çeşitli performans ölçütleri kullanılarak değerlendirilmiştir. Değerlendirme sonucuna göre, LR yöntemi DIS Flooding saldırı tespitini daha yüksek başarım ile gerçekleştirmiştir.

Anahtar Kelimeler: DIS Flooding, Makine Öğrenmesi, Nesnelerin İnterneti, RPL, Saldırı Tespiti.

1. Introduction

A new networking architecture known as the Internet of Things (IoT) offers to make life easier and more comfortable by transforming every physical object inside our surroundings into a smart object capable of sensing the environment and communicating with the other smart things in the network. IoT has contained some components such as sensors-actuators, identifiers, software, and wireless network technology [1].

- Sensors-actuators: to gather information from the network environment.

- Identifiers: identifying the data source

- Software: analyzing data

- Wireless network technology: to inform and communicate

A rapidly growing number of sensors, actuators, and smart devices connected to the Internet have gained acceleration to IoT. Specifically, it allows gathering information and remote control of real objects through the internet, thereby integration between real-world and computer-based systems and leads to better reliability, accuracy, and financial benefits. However, the increasing number of devices and their integration with the network environment has attracted many security risks [2]. The security risks can be extremely dangerous for sensitive information. Especially cyber attacks have occurred in big enterprises so an attacker can steal company reports, credit card information, and users' privacy documents.

IoT security is an important issue for the network system's sustainability. It can be exposed to the destructive effects of attacks due to the inconvenience of the limited resource structure. As IoT devices become commonly used and their number increases, the attacks targeting IoT devices are expected to grow in the future.

Routing protocol for Low Power and Lossy Networks (LLNs) (RPL) is the most important routing protocol for Internet Protocol version 6 (IPv6) based Low-power Wireless Personal Area Networks. There have been occurred many cyber-attacks to the tremendous quantity of IoT applications and their integration services via the internet. The most common RPL attacks directly target nodes' resource consumption in the IoT environment. Thus, IoT has to overcome the negative effects of cyberattacks such as the massive loss of data packets, heavy computational load, and node's energy consistency for LLNs.

The remainder of this article is divided into four sections: Section 2 provides a detailed discussion on IoT network security, attack types, and attack detection approaches. Section 3 gives an overview of scenarios, IoT network design, and simulation. Section 4 presents the effectiveness of the network according to scenarios, the detection of the DIS Flooding attacks using Logical Regression (LR) and Support Vector Machine (SVM) methods, and the performance comparison of these methods. Finally, Section 5 concludes achieved objectives and future works.

2. Related Works and Background

Some machine learning algorithms have been used to detect various attacks directly related to constrained energy sources such as Distributed Denial of Service (DDoS), Hello flooding, and Sybil attacks. Attack detection studies on RPL-based IoT networks in the scientific literature are listed in Table 1.

Table 1. Recent related works

Reference	**Type of Attack**	**Method**	**Detection Rate (%)**
[3]	DDoS	K-Means Expectation-Maximization	76.36 80.51
[4]	Hello flooding	Gated Recurrent Unit SVM LR	99.8 99 98.95
[5]	DDoS	Random Forest	above 96
[6]	DDoS	Optimized SVM SVM	97.6 89.8
[7]	DDoS	Multiple Linear Regression	97.86
[8]	DDoS	Artificial Neural Networks	98
[9]	Hello flood, DIS, increased version, and decreased rank	Random Forest Naïve Bayes	99.33 96.7
[10]	Sybil	SVM LR Decision Tree Random Forest	93 84 83 79
[11]	Sybil	A novel Artificial Bee Colony-inspired detection algorithm	average 95
[12]	Version number Hello flooding Blackhole	Kernel Density Estimation	96 90 68
This article	DIS flooding	LR SVM	99.16 96.92

In the literature, many different types of IoT attacks have been detected with over 80% accuracy, but an efficient and suitable solution has not been proposed yet for DIS flooding attacks against RPL [2], [13]. In this study, it is aimed to decrease the power consumption of the nodes in the IoT network and thus improve the efficiency of the network by detecting DIS flooding attacks.

3. Materials and Method

3.1. DODAG Buildings and Design

RPL is a standard routing protocol based on IPv6. IoT devices, which are using RPL, communicate with a particular topology that unifies mesh and tree topologies known as Destination Oriented Directed Acyclic Graphs (DODAG). A DODAG starts with a sink node which is a root node. RPL defines three control messages for sharing routings information of nodes and control DODAGs: DODAG Information Object (DIO), DODAG Advertisement Object (DAO), and DODAG Information Solicitation (DIS) messages.

The network topologies designed for a normal network (without any malicious nodes) and a network with a malicious node sending DIS message periodically are presented in Fig. 1(a) and Fig. 1(b), respectively.

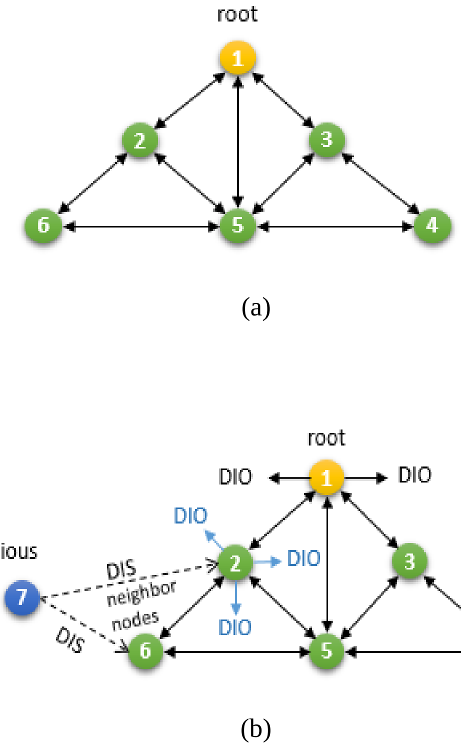

Fig. 1. The network topologies scenarios: (a) before DIS flooding attack, (b) when DIS Flooding attack happened

Nodes utilize DIS messages to join the IoT network in RPL. A malicious node sends continuously the floods of DIS message to its nearby nodes until it gets a DIO message in order to join an existing DODAG. This situation increases power consumption and causes latency and high computational load [2].

3.2. Proposed Methodology

Nodes (Skymote) are added into the simulator environment according to the scenario and the IoT network is built. The contents of the message packets sent by the nodes are captured and filtered. After simulation, all data is exported to an Excel file. The features required for the total energy consumption are extracted and a dataset is generated for attack detection using machine learning methods. The dataset is then normalized and divided into two subsets: the training and test datasets. Attacks are detected by machine learning algorithms and nodes are classified as “normal” and “malicious”. The workflow of the proposed model in this study for DIS Flooding attack detection is given in Fig 2.

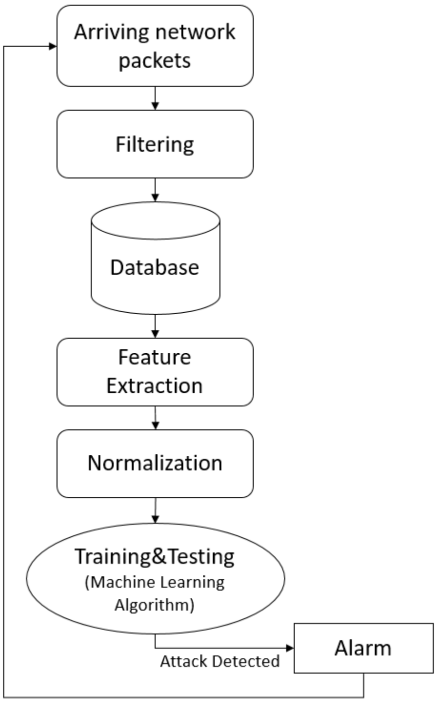

Fig. 2. The workflow of DIS Flooding attack detection and prevention

In the study, the networks before the DIS flooding attack and during the attack have been simulated using Contiki-Cooja. Node identification (ID), Central Processing Unit (CPU), Low Power Mode (LPM), transmit (Tx), receive (Rx) and total energy (TE) features have been selected from the simulation data and then the data have been normalized. Min-max normalization, which is the most popular method, has been used for scaling the selected features. The normalized data have been divided into a 80:20 ratio for training and test processes. SVM and LR algorithms are used for attack detection.

4. Simulation Results and Performance Evaluation

In this study, DIS Flooding attacks have been detected with LR and SVM machine learning algorithms, which are widely used in the literature. In order to train the SVM and LR algorithms and to analyze the impact of the DIS flooding attacks on the network, a simulation scenario including a malicious node has been created as given in Table 2.

Table 2. A simulation scenario of DIS Flooding attack

Parameter	Scenario
Total number of nodes	5
Number of sink nodes	1
Number of normal nodes	3
Number of DIS flooding attacker nodes	1

Based on the scenario, the network is simulated for 15 minutes of simulation time. The obtained simulation data consists of ID, CPU, LPM, Tx, Rx, and TE numerical values calculated for each node during the simulation and then normalized using the standard min-max normalization.

The performance of LR and SVM methods is evaluated in terms of accuracy, recall, precision, Mathew Correlation Coefficient (MCC), F1-score, Area under Receiver Operating Characteristic (ROC) curve (AUC), and Cohen's Kappa. Evaluation results are given comparatively in Table 3.

Table 3. The performance comparison of SVM and LR methods

Metric	LR	SVM
Accuracy	0.99	0.97
Precision	1.00	1.00
Recall	0.96	0.87
F1-score	0.98	0.93
MCC	0.98	0.92
Cohen's kappa	0.97	0.91
Roc_auc	0.98	0.93

LR has provided a better accuracy rate of 99.16% under the DIS Flooding attacks. According to the obtained results, both SVM and LR algorithms have presented the highest precision value of 1.00. The other performance metrics indicate that the LR algorithm is more successful results than SVM in the detection of DIS flooding attacks.

5. Conclusion

IoT devices generally have constrained memory and limited processing capabilities. Therefore, DIS Flooding attacks can easily exhaust their resources. In this study, a machine learning-based attack detection approach has been presented to detect DIS Flooding attacks in IoT network security. LR and SVM have achieved classification accuracy of 99.16% and 96.92%, respectively. Although LR and SVM have presented significant results within the scope of this study, some improvements are needed for network security, such as prevention and mitigation of the attacks. So in the future study, we will address how to effectively mitigate and isolate DIS Flooding attacks in RPL networks.

References

[1] A. Rayes, S. Salam, Chapter 1 Internet of Things (IoT) Overview, *Internet of Things From Hype to Reality*, Springer Nature Switzerland AG, pp. 1-35, 2019. https://doi.org/10.1007/978-3-319-99516-8_1

[2] A. Verma and V. Ranga, "Mitigation of DIS flooding attacks in RPL-based 6LoWPAN net-works," *Trans Emerging Tel Tech.*, vol. 31(2), e3802, pp. 1-25, 2020. https://doi.org/10.1002/ett.3802

[3] V. Odumuyiwa and R. Alabi, "DDOS Detection on Internet of Things Using Unsupervised Algorithms", Journal of Cyber Security and Mobility, vol. 10, no. 3, pp. 569-592, 2021. https://doi.org/10.13052/ jcsm2245-1439.1034

[4] S. Cakir, S. Toklu, and N. Yalcin, "RPL Attack Detection and Prevention in the Internet of Things Networks Using a GRU Based Deep Learning," *IEEE Access*, vol. 8, pp. 183678-183689, 2020. https://doi.org/10.1109/ACCESS.2020.3029191

[5] F. S. De Lima Filho, F. A. F. Silveira, A. De Medeiros Brito Junior, G. Vargas-Solar, and L. F. Silveira, "Smart Detection: An Online Approach for DoS/DDoS Attack Detection Using Machine Learning," Security and Communication Networks, vol. 2019, pp. 1-15, 2019. https://doi.org/10.1155/2019/1574749

[6] R. Abubakar, A. Aldegheishem, M. Majeed, A. Mehmood, N. Alrajeh, and M. Carsten, "An Effective Mechanism to Mitigate Real-time DDoS Attack Using Dataset", *IEEE Access*, vol. 8, pp. 126215-126227, 2020. https://doi.org/10.1109/ACCESS.2020.2995820

[7] S. Sambangi and L. Gondi, "A Machine Learning Approach for DDoS (Distributed Denial of Service) Attack Detection Using Multiple Linear Regression," in *Multidisciplinary Digital Publishing Institute Proc.*, vol. 63, p. 51, https://doi.org/10.3390/proceedings2020063051

[8] A. Saied, R. E. Overill, and T. Radzik, "Detection of known and unknown DDoS attacks using Artificial Neural Networks," *Neurocomputing*, vol. 172, pp. 385-393, 2016. https://doi.org/ 10.1016/j.neucom.2015.04.101

[9] M. Sharma, H. Elmiligi, F. Gebali, and A. Verma, "Simulating Attacks for RPL and Generating Multi-class Dataset for Supervised Machine Learning," in *2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, pp. 20-26, 2019. https://doi.org/10.1109 /IEMCON.2019.8936142

[10] M. Mounica, R. Vijayasaraswathi, and R. Vasavi, "Detecting Sybil Attack in Wireless Sensor Networks Using Machine Learning Algorithms," in *IOP Conference Series: Materials Science and Engineering*, vol. 1042, no. 1, p. 012029, 2021. https://doi.org/ 10.1088/ 1757-899X/1042/1/012029

[11] S. Murali and A. Jamalipour, "A Lightweight Intrusion Detection for Sybil Attack Under Mobile RPL in the Internet of Things," *in IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 379-388, Jan. 2020, https://doi.org/10.1109/JIOT.2019.2948149

[12] N. Müller, P. Debus, D. Kowatsch, and K. Böttinger, ''Distributed anomaly detection of single mote attacks in RPL networks,'' in *Proc. 16th Int. Joint Conf. e-Bus. Telecommun.*, vol. 2, pp. 378-385, 2019. https://doi.org/10.5220/0007836003780385

[13] A. Mayzaud, R. Badonnel, and I. Chrisment, "A taxonomy of attacks in RPL-based Internet of Things", *International Journal of Network Security*, vol. 18, no. 3, pp. 459-473, 2016. https://doi.org/10.6633/ IJNS.201605.18(3).07