www.dergipark.gov.tr
ISSN:2148-3736
El-Cezerî Fen ve Mühendislik Dergisi
Cilt: 9, No: 4, 2022 (1529-1541)

El-Cezerî Journal of Science and Engineering
Vol: 9, No: 4, 2022 (1529-1541)
DOI : 10.31202/ecjse.1149925

ECJSE

Research Paper / Makale

A Novel Approach to Prevention of Hello Flood Attack in IoT Using Machine Learning Algorithm

Serkan GÖNEN [1a], Mehmet Ali BARIŞKAN[1b], Gökçe KARACAYILMAZ[2c], Birkan ALHAN[1d],

Ercan Nurcan YILMAZ[3e], Harun ARTUNER[2f], Erhan SİNDİREN [3g]

[1] Istanbul Gelisim University, Faculty of Engineering and ArchitectureI, stanbul, Turkey
[2] Hacettepe University, Faculty of Engineering, Ankara, Turkey
[3] Gazi University, Faculty of Technology, Ankara, Turkey
enyilmaz@gazi.edu.tr

Received/Geliş: 28.07.2022 **Accepted/Kabul:** 30.11.2022

Abstract: With the developments in information technologies, every area of our lives, from shopping to education, from health to entertainment, has transitioned to the cyber environment, defined as the digital environment. In particular, the concept of the Internet of Things (IoT) has emerged in the process of spreading the internet and the idea of controlling and managing every device based on IP. The fact that IoT devices are interconnected with limited resources causes users to become vulnerable to internal and external attacks that threaten their security. In this study, a Flood attack, which is an important attack type against IoT networks, is discussed. Within the scope of the analysis of the study, first of all, the effect of the flood attack on the system has been examined. Subsequently, it has been focused on detecting the at-tack through the K-means algorithm, a machine learning algorithm. The analysis results have been shown that the attacking mote where the flood attack has been carried out has been successfully detected. In this way, similar flood attacks will be detected as soon as possible, and the system will be saved from the attack with the most damage and will be activated as soon as possible.

Keywords: IoT, Cyber Security, IoT Security, Flood Attacks, Machine learning

Makine Öğrenmesi Algoritmasını Kullanarak IoT'de Hello Flood Saldırısının Önlenmesine Yönelik Yeni Bir Yaklaşım

Öz: Bilgi teknolojilerindeki gelişmelerle birlikte alışverişten eğitime, sağlıktan eğlenceye hayatımızın her alanı dijital çevre olarak tanımlanan siber ortama geçiş yapmıştır. Özellikle internetin yaygınlaşmasıyla ve her cihazın IP tabanlı olarak kontrol edilmesi ve yönetilmesiyle Nesnelerin İnterneti (IoT) kavramı ortaya çıkmıştır. IoT cihazlarının sınırlı kaynaklarla birbirine bağlı olması, kullanıcıların güvenliklerini tehdit eden iç ve dış saldırılara karşı savunmasız kalmasına neden olur. Bu çalışmada, IoT ağlarına karşı önemli bir saldırı türü olan Flood saldırısı ele alınmıştır. Çalışmanın analizi kapsamında öncelikle flood saldırısının sistem üzerindeki etkisi incelenmiştir. Ardından, bir makine öğrenmesi algoritması olan K-means algoritması aracılığıyla saldırıyı tespit etmeye odaklanılmıştır. Analiz sonuçları, flood saldırısının gerçekleştirildiği saldırı noktalarının başarıyla tespit edildiğini göstermiştir. Bu sayede benzer flood saldırıları en kısa sürede tespit edilecek ve sistem, saldırıdan en az hasarla kurtulacak ve en kısa sürede devreye girecektir.

Anahtar Kelimeler: IoT, Siber Güvenlik, IoT Güvenliği, Flood Saldırıları, Makine öğrenmesi

How to cite this article
Gonen, S., Bariskan, M. A., Karacayilmaz, G., Alhan, B., Yilmaz, E. N., Artuner, H., Sindiren, E., "A Novel Approach to Prevention of Hello Flood Attack in IoT Using Machine Learning Algorithm", El-Cezerî Journal of Science and Engineering, 2022, 9(4), 1529-1541.

Bu makaleye atıf yapmak için
Gönen, S., Barışkan, M. A., Karacayılmaz, G., Alhan, B., Yılmaz, E. N., Artuner, H., Sindiren, E., "Makine Öğrenmesi Algoritmasını Kullanarak IoT'de Hello Flood Saldırısının Önlenmesine Yönelik Yeni Bir Yaklaşım", El-Cezerî Fen ve Mühendislik Dergisi 2022, 9(4), 1529-1541.

ORCID ID: [a]0000-0002-1417-4461; [b]0000-0002-8039-2686; [c]0000-0001-8529-1721; [d]0000-0003-1511-0109; [e]0000-0001-9859-1600; [f]0000-0002-6044-379X; [g]0000-0003-1138-1913

1. Introduction

The history of humanity has passed through important stages that shape human life. Although these stages are divided into many different types of categories, they can basically be divided into three basic stages that affect social life. The first is the agricultural society, the second is the industrial society, and finally, the information society. The information society we live in has led to significant changes in human life with the joint use of information systems and the concept of networks. The introduction of the "Internet," the largest network, into our lives. From banking to shopping, from health services to education, all areas have witnessed the digital transformation. With the development of this process, the meaning of the internet concept in our lives is also changing. To facilitate human life, the concept of the Internet of Things has entered our lives with the connection of our devices to the internet in daily life.

The Internet of Things has become one of the most popular technologies in recent years. Control mechanisms of devices are developed by using microprocessors in many areas such as health institutions, small household appliances, and machines used in factories. These environments are based on smart devices that receive data from the real world, then process and transmit this data to computing centers, produce some information-based services and take the necessary actions [1]. The Internet of Things (IoT) can be seen as an evolution in connecting these microprocessor-integrated devices to the internet.

With the popularity of the internet of things technology in recent years, many research studies have also been its subject. The internet of things, which is foreseen to be used in many fields such as logistics, transportation, wearable technology, smart devices, smart agriculture, smart health care, is expected to be integrated into 75 billion different devices by 2025 [2]. The McKinsey Global Institute predicts that the internet of things will reach $11 trillion economically by 2025, with a large part of it in business and industrial applications [3, 4]. With this development of the internet of things sector, the system's security is also becoming a very important issue. Still, in such a growing sector, the problem of security analysis is not adequately addressed. Although IoT devices make our daily tasks quick and simple by making our lives easier, they also have high-security flaws. The current inadequate security measures implemented to defend smart devices cause people to not benefit from IoT systems sufficiently. In particular, resource and power consumption limitations specific to IoT devices make this vulnerability one of the important targets of attackers who want to exploit it.

In this study, to increase IoT security, the Flood attack, which is one of the important attacks against such systems, has been examined, and a machine learning-based attack detection method has been developed.

2. Related Work

Humanity traveled a long time from wheel to the car, but little time passed from car to space travel. With the invention of controllers, smart devices started to become part of our lives. From our factories to our electric grid, from traffic lights to smartwatches, all these devices have become mini-computers; with this development, the importance of communication between these devices has become one of the industry's most critical needs. With this paradigm, the internet becomes the platform of these communications [5]. Due to the development of Internet of Things (IoT) technology, versatile inventor Nikola Tesla's prediction of realizing a "global brain" comes true with interdisciplinary innovations [6]. These devices control and work as planned heavily depending on effective data communication protocols [7]. As important as these communications become, attacks on those IoT applications become attractive [8]. For that reason, the security of

these devices, especially those used in critical infrastructures, has become one of the most important parts of IoT technology. As an example of IoT systems' lack of security precaution, we can use IP cam systems [9]. As of 2021, Open port search on Shodan Search Engine (port:554 has_screenshot: true) gives 95722 results without security measurements. Machine learning tools are used in many IoT ecosystems for security [9, 10]. However, it faces challenges from security to data analysis that adversaries can take loopholes to hack these systems through tampering history data [11]. Indeed, remotely managed IoT devices equipped with various cyber and physical interfaces create new attack capabilities. They can bridge different and possibly separated networks and technologies and interact unexpectedly by expanding or abusing their cyber-physical interactions. Worse still, the lack of security certification in IoT increases the vulnerability surface and available connectivity paths. Traditional risk assessment methodologies fail to capture this new and evolving threat landscape [12]. One of the biggest problems for IoT devices in terms of security is DDoS attacks. On larger systems, Botnets can be used to carry out such cyber attacks [6].

Properties of an IoT system security can be investigated in 5 integral points. These are Mobility, Wireless Communication, Embedded Use, Diversity of Components, and Scalability. Every IoT system is connected with a mobile app and connected to the internet via many providers. So Security Systems must check these connections. IoT devices generally relate to the internet via many wireless links, including Blue- tooth, 802.11, WiMAX, Zigbee, etc. Exposing wireless signals in public-eye frequency has been a security concern in recent years. So security systems must take control of these connections and check security measures as most Major IoT devices have a single functionality. Accordingly, the detection of patterns in data transmission is often presented in a unique model and can be considered a potential vulnerability. Therefore, security systems must take these patterns into account and control the flow of information. There is a wide range of inconsistencies in terms of connected devices type and topology in the IoT. Privacy designs must accommodate even the simplest of devices. The number of connected devices is growing dramatically day by day, and IoT clients cannot monitor the privacy of their data under the computation of these devices [13]. While some articles about the security of IoT devices use machine learning algorithms to pre-record data sets [14], In this article, we use real-time traffic to analyze and detect attacks in the systems.

Within the scope of studies carried out within the scope of IoT attacks, Singh et al. proposed an advanced hybrid intrusion detection system by combining multi-layer perceptron neural network and fuzzy logic to detect hello flood attacks in their research. Their proposed system used signal strength and distance information to detect the hello flood attack [15]. Çakır et al. proposed a deep learning system based on the Gated Recurrent Unit model to detect and prevent Hello Flood attacks on the RPL protocol used on IoT networks [16]. In the study by Ioulianou et al., they proposed a hybrid lightweight signature-based IDS system in order to mitigate the attacks, especially in the hello flood type, in the DDoS attack. Their work performed a simulation on Contiki OS and showed an approach with IDS architecture against intrusions in the network [17]. Another study that conducted attack analysis on Contiki OS was carried out by Razaa et al. In the study; they proposed a real-time intrusion detection system called SVELTE. SVELTE was a system embedded in the border router in 6LoWPAN networks. The purpose of the system was to detect intrusions and filter malicious traffic by analyzing collected information about the RPL protocol [18].

In the research by Shreenivas et al., the ETX (Expected Transmissions) measure was used to detect malicious activities in 6LoWPAN networks. They proposed a geographical clue to detect malicious nodes attacking the network [19]. The study by Napiah et al. used CHA-IDS (compression header analyzer intrusion detection system) to detect and analyze routing attacks. The study used the best-first search algorithm in the network traffic generated with the Cooja simulator. The six machine learning algorithms were used to achieve the best performance. The values obtained from the

research were compared in terms of energy and power consumption statistics for 6LoWPAN networks [20].

Yavuz et al. investigated a deep learning-based machine learning method for attack detection in IoT networks. In the study, a combination of random forests, histogram, and Pearson correlation coefficient was used to improve performance on the data set. They simulated this created dataset by comparing it with the UNSW-NB15 and KDDCUP99 datasets [21]. Jan et al. proposed a lightly supervised machine learning-based Support Vector Machine (SVM) to detect an attacker trying to inject redundant data into the IoT network [22].

This study used central mote and remote motes representing IoT devices such as heat, humidity, pressure, and one attacker mode in the attack analyses considering a smart factory model. The effects of the attack on the system have been demonstrated by using various tools through both power consumption and packet analysis. Finally, as a result of the analysis of the traffic logs obtained from the reference model without the attacker and the model with the attacker, the attacker mote has been successfully detected through the machine learning algorithm. K-means algorithm is used in the study. Artificial intelligence algorithms need high system resources to work fast. Here, by using the K-Means algorithm, it has been tried to add a different perspective to the literature by providing high-speed results with low system resources with an unsupervised structure. The study focused on the IoT Flood attack, but by following the steps of the flow diagram described in detail in Figure 3, the study can be used to detect and prevent other types of attacks. With the detection ability gained in the study, it will be possible to detect new vulnerabilities in the system, close it as soon as possible, or save the system by intervening with the least damage. It is thought that the study will make significant contributions to the detection of IoT attacks and vulnerabilities.

3. Testbed

The study used the Cooja simulator and Foren6 6LoWPAN network analysis tool on the Contiki operating system to simulate the hello flood attack. Within the scope of the analysis of the study, first of all, a network model has been created on the Contiki simulator. One central mote, 50 standard motes, and one attacker mote have been created on the created network model. A large part of the Internet of Things consists of wireless transceivers combined with sensors that can be found in almost everything physical - devices, clothing, machines, buildings. The phrase "wireless transceiver coupled with sensors" in question is somewhat cumbersome to use, so such a node of the IoT is called a mote (short for remote control). Standard motes on the topology use the central node to transfer communication to external networks. The purpose of the attacker mote on the simulation is to increase the battery consumption on the standard and central mote by sending hello packets continuously to the network. As a result of this traffic, it is aimed that other motes try to respond to the packets from the attacker motes, preventing them from doing the tasks they are responsible for and rendering the motes unusable.

Figure 1 and Figure 2 show the network map used in the hello flood simulation. Figure 1 represents the reference model, while Figure 2 shows the network map with the attacking node.

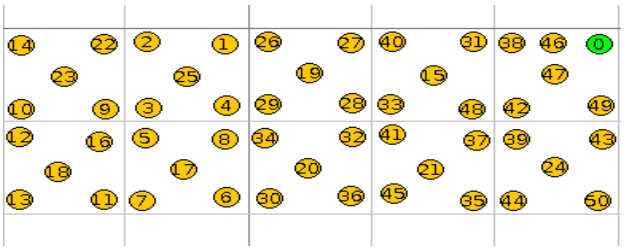


Figure 1. Network Map (Without Attacker Mote)

The green mote on the top of the figure represents the central mote, the yellow motes the standard motes, and the purple mote represents the attacker mote. At the time of the attack, the attacking mote, which is located within the transmission capacity of the central mote, transmits hello packets to other motes on the network. The attack has been successfully carried out as the other motes reached by the transmitted hello packets returned the reply packet to the mote from which the packet came.

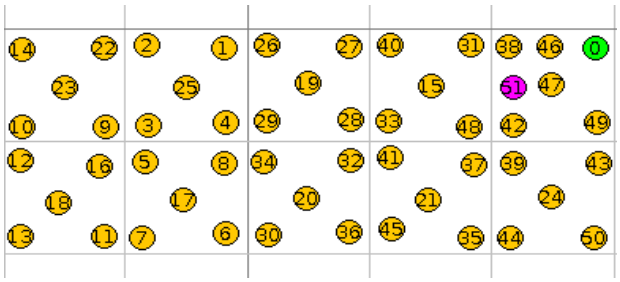


Figure 2. Network Map (With Attacker Mote)

All devices in the network map send packets to communicate among themselves. Wireshark has been used to monitor, record, and examine the communication between the nodes in the scenario realized on the simulation.

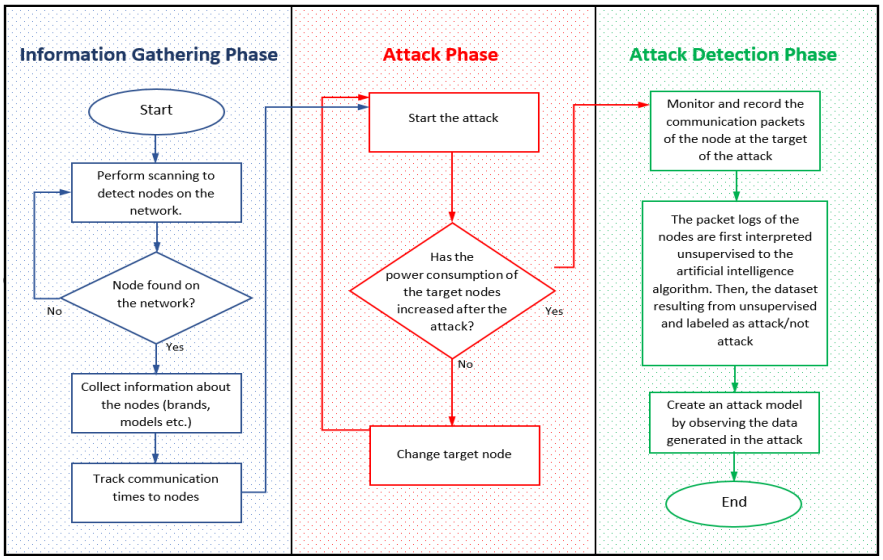


Figure 3. IoT Hello Flood Flowchart

As depicted in Figure 3 flowchart, the Hello flood attack consists of 3 stages. In the first stage, the attack information gathering stage, the network is scanned, and the nodes are detected. After collecting information about the detected nodes, the network traffic is examined, and the central node is determined. In the second stage, the hello flood attack is initiated, and hello packets are sent over the network by the attacking node. As a result of the intensity of the attack packets sent, the increase in the communication times of other nodes and the battery consumption status are monitored. In the last stage, which is the attack detection stage, the network traffic is logged. The machine learning algorithm processes the logged network traffic, and attack detection is provided. In this way, it is ensured that the damage to the system is prevented.

4. Flood Attack and Analysis Result

The attack scenario was carried out on a fixed network with wireless network sensors. For this reason, analysis and machine learning integration can be performed on insider or external attacks

that will occur on a fixed network. In this section, the attack values depicted in Figure 5 have been compared with the reference values shown in Figure 4, where there was no attack. In this way, the effects of the attack on IoT devices have been examined.

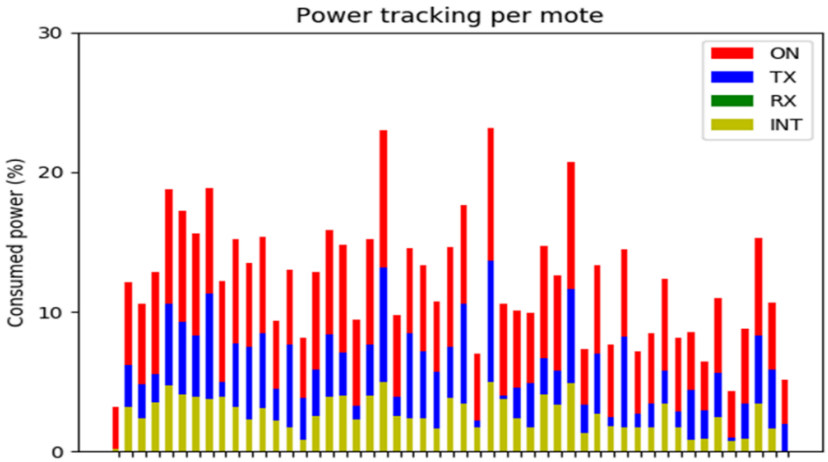


Figure 4. Power Consumption Graph (Reference Model)

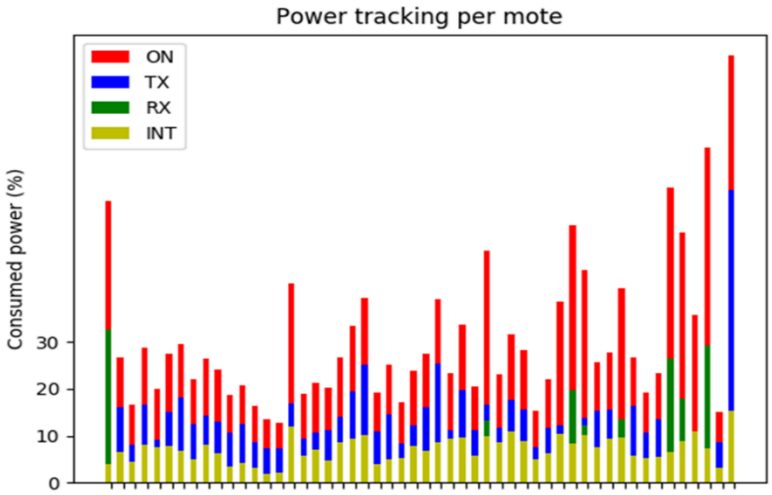


Figure 5. Power Consumption Graph (After Flood Attack)

When Figure 4 and Figure 5 are examined, ON values show the power consumption of the node devices when they are turned on. INT values represent the interference value of the nodes. This value can be interpreted as the communication density between nodes. In Figure 4, when the node devices are ON, their power consumption is around 20 percent, while the interference values are around 5 percent. On the other hand, in Figure 5, when the node devices are ON, their power consumption is around 40-50 percent. It has been observed that the interference values have increased in the nodes close to the attacking node.

The test environment has been run on the Destination Oriented Directed Acyclic Graph (DODAG) network. Network communication in the DODAG structure must be terminated on the root node. In this context, the late communication of the root node is a costly loss on this network. When the pcap logs on the DODAG network are examined over Wireshark, it is understood that the graphical explanations in Figure 4 and Figure 5 are supported. Figure 6 belongs to the time when the attacking mote is not in the DODAG network, and Figure 7 belongs to the scenario where the attacking mote has carried out a hello flood attack on the network. Packets analyzed with Wireshark are shown in Figure 6 and Figure 7. When Figure 6 and Figure 7 are compared, it is seen that while the communication traffic occurring at the same time is 149471 packets in the reference network,

515813 packets are in transmission in the attack scenario. In addition, it is seen that 84.3 percent of the packets in the attack scenario belong to the packets sent from and received by the attacker mote. These values show the effect of the Flood attack on IoT networks where power consumption is very critical.

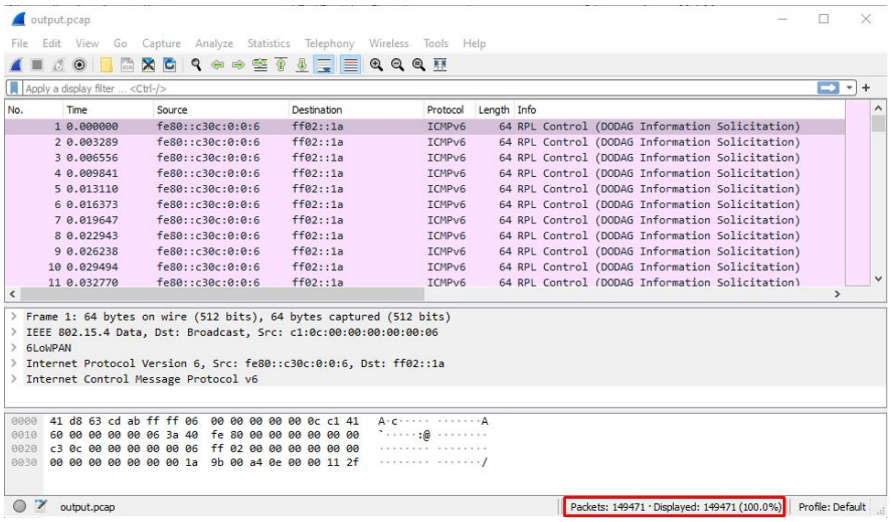


Figure 6. Network Packet Analysis (Reference Model)

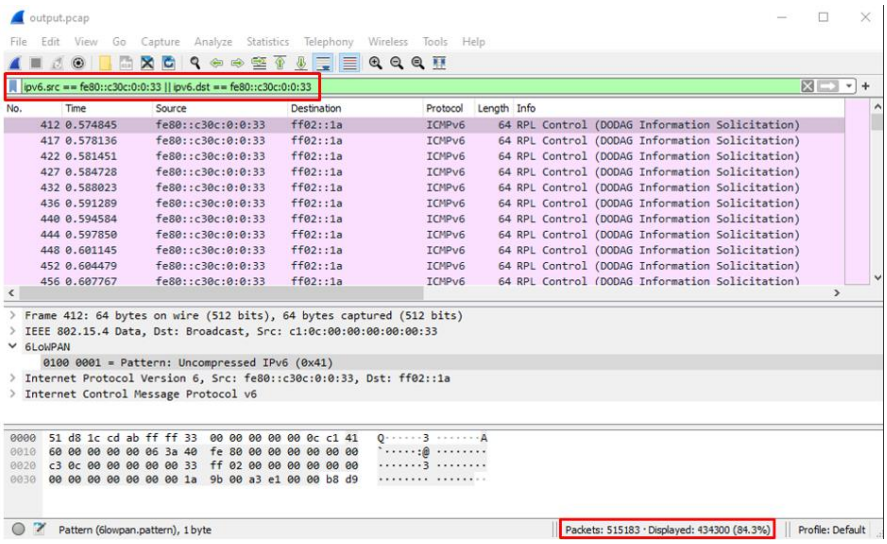


Figure 7. Network Packet Analysis (Post Flood Attack)

As a result, when the attacker mote was included in the network, all traffic was disrupted. In this case, power consumption and system flow in wireless sensor networks (WSN) will differ from the system's norms. For example, in a data center, servers must be kept at certain temperatures. Wireless sensor networks are activated when the temperature drops below or above a certain level and trigger the planned system. As a result of the trigger, the data center is kept at the required temperature level. However, an attacker node entering this wireless sensor network may face catastrophic risks such as data centerfire. It will delay the communication of the root node in this system and the triggering of the system that is planned to work.

In the second phase of the analysis, the network traffic of the reference and attack scenarios has been analyzed with the Foren6 6LoWPAN network analysis tool. Foren6 application is an open source IoT network analysis application that allows real-time or post-analysis and inspection on network packets.

As a result of the analysis, it can be seen in the Figure 8 and Figure 9 that although the Attacker mote sent 1501 packets, the Root mote only sent 113 packets. In addition, when the attacker is not present, the total number of control and data packets is 2015, while the network traffic with the attacker is examined, it is seen that the total number of packets has increased to 5956.

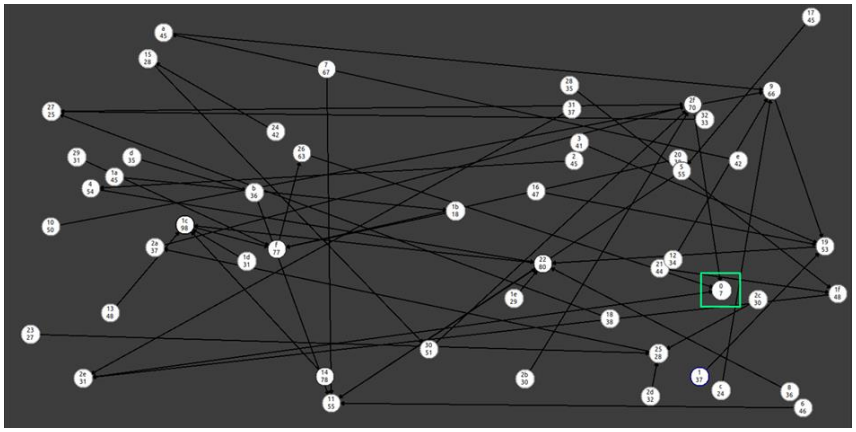


Figure 8. Network Analysis with A 6LoWPAN Diagnosis Tool (Without Attacker)

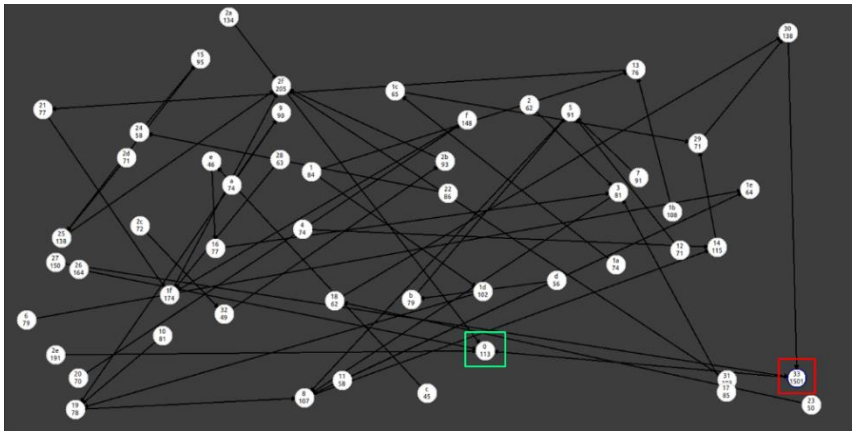
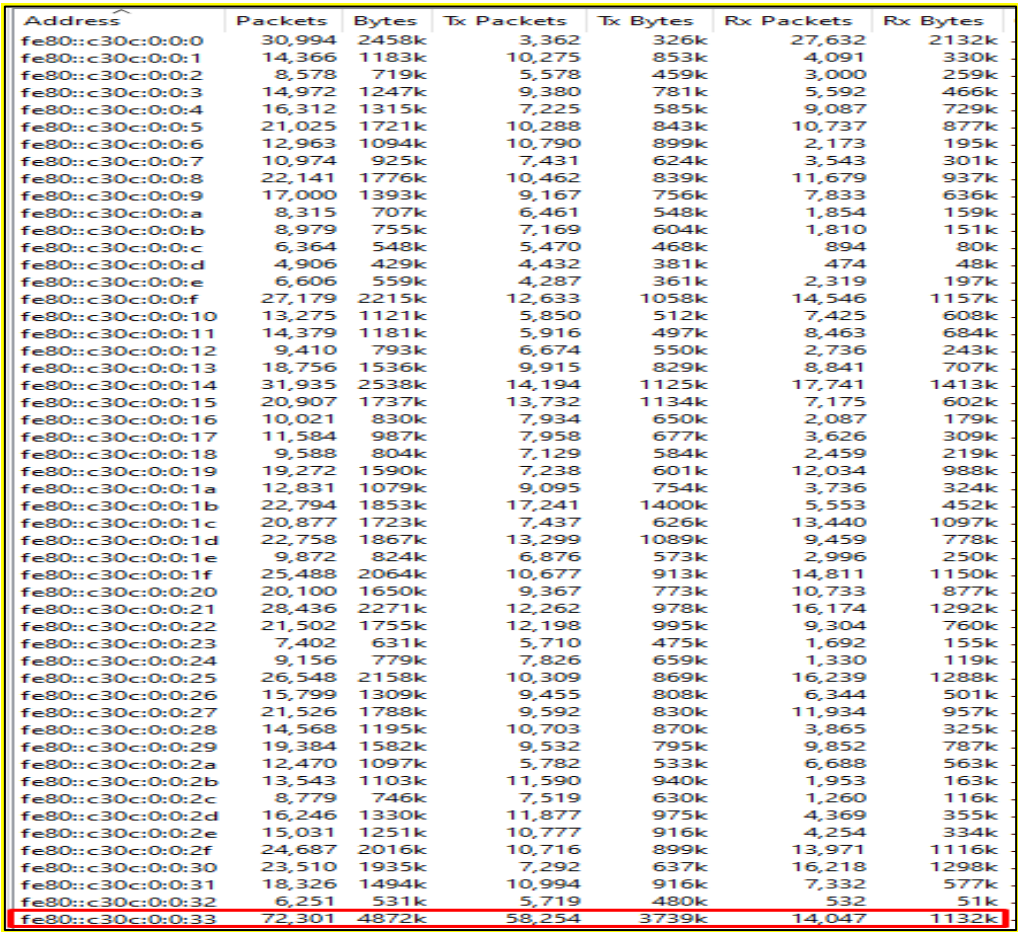


Figure 9. Network Analysis with A 6LoWPAN Diagnosis Tool (With Attacker)

5. Attack Analysis via Machine Learning

To prevent IoT Systems from being affected by existing attacks or to eliminate the attack with the least damage, the detection of the attacks carried out within the scope of the analysis scenarios should be done as soon as possible. In this context, within the scope of the study, machine learning analysis is proposed to detect attacks with a heuristic approach.

The pcap file, which has been logged without an attacking mote on the network created by machine learning analysis, has been used as a reference dataset. In this way, the machine learning learns the network norm traffic on the target system without the attacker. The attacking mote is constantly sending hello packets to manipulate network traffic. In this respect, if the packets sent by the devices on the network are monitored and logged for a certain period, it will be possible to understand which device is the attacker. Regarding this situation, the number of packets and data information sent by the attacking mote and other motes on the network traffic is shown in Figure 10.



Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
fe80::c30c:0:0:0	30,994	2458k	3,362	326k	27,632	2132k
fe80::c30c:0:0:1	14,366	1183k	10,275	853k	4,091	330k
fe80::c30c:0:0:2	8,578	719k	5,578	459k	3,000	259k
fe80::c30c:0:0:3	14,972	1247k	9,380	781k	5,592	466k
fe80::c30c:0:0:4	16,312	1315k	7,225	585k	9,087	729k
fe80::c30c:0:0:5	21,025	1721k	10,288	843k	10,737	877k
fe80::c30c:0:0:6	12,963	1094k	10,790	899k	2,173	195k
fe80::c30c:0:0:7	10,974	925k	7,431	624k	3,543	301k
fe80::c30c:0:0:8	22,141	1776k	10,462	839k	11,679	937k
fe80::c30c:0:0:9	17,000	1393k	9,167	756k	7,833	636k
fe80::c30c:0:0:a	8,315	707k	6,461	548k	1,854	159k
fe80::c30c:0:0:b	8,979	755k	7,169	604k	1,810	151k
fe80::c30c:0:0:c	6,364	548k	5,470	468k	894	80k
fe80::c30c:0:0:d	4,906	429k	4,432	381k	474	48k
fe80::c30c:0:0:e	6,606	559k	4,287	361k	2,319	197k
fe80::c30c:0:0:f	27,179	2215k	12,633	1058k	14,546	1157k
fe80::c30c:0:0:10	13,275	1121k	5,850	512k	7,425	608k
fe80::c30c:0:0:11	14,379	1181k	5,916	497k	8,463	684k
fe80::c30c:0:0:12	9,410	793k	6,674	550k	2,736	243k
fe80::c30c:0:0:13	18,756	1536k	9,915	829k	8,841	707k
fe80::c30c:0:0:14	31,935	2538k	14,194	1125k	17,741	1413k
fe80::c30c:0:0:15	20,907	1737k	13,732	1134k	7,175	602k
fe80::c30c:0:0:16	10,021	830k	7,934	650k	2,087	179k
fe80::c30c:0:0:17	11,584	987k	7,958	677k	3,626	309k
fe80::c30c:0:0:18	9,588	804k	7,129	584k	2,459	219k
fe80::c30c:0:0:19	19,272	1590k	7,238	601k	12,034	988k
fe80::c30c:0:0:1a	12,831	1079k	9,095	754k	3,736	324k
fe80::c30c:0:0:1b	22,794	1853k	17,241	1400k	5,553	452k
fe80::c30c:0:0:1c	20,877	1723k	7,437	626k	13,440	1097k
fe80::c30c:0:0:1d	22,758	1867k	13,299	1089k	9,459	778k
fe80::c30c:0:0:1e	9,872	824k	6,876	573k	2,996	250k
fe80::c30c:0:0:1f	25,488	2064k	10,677	913k	14,811	1150k
fe80::c30c:0:0:20	20,100	1650k	9,367	773k	10,733	877k
fe80::c30c:0:0:21	28,436	2271k	12,262	978k	16,174	1292k
fe80::c30c:0:0:22	21,502	1755k	12,198	995k	9,304	760k
fe80::c30c:0:0:23	7,402	631k	5,710	475k	1,692	155k
fe80::c30c:0:0:24	9,156	779k	7,826	659k	1,330	119k
fe80::c30c:0:0:25	26,548	2158k	10,309	869k	16,239	1288k
fe80::c30c:0:0:26	15,799	1309k	9,455	808k	6,344	501k
fe80::c30c:0:0:27	21,526	1788k	9,592	830k	11,934	957k
fe80::c30c:0:0:28	14,568	1195k	10,703	870k	3,865	325k
fe80::c30c:0:0:29	19,384	1582k	9,532	795k	9,852	787k
fe80::c30c:0:0:2a	12,470	1097k	5,782	533k	6,688	563k
fe80::c30c:0:0:2b	13,543	1103k	11,590	940k	1,953	163k
fe80::c30c:0:0:2c	8,779	746k	7,519	630k	1,260	116k
fe80::c30c:0:0:2d	16,246	1330k	11,877	975k	4,369	355k
fe80::c30c:0:0:2e	15,031	1251k	10,777	916k	4,254	334k
fe80::c30c:0:0:2f	24,687	2016k	10,716	899k	13,971	1116k
fe80::c30c:0:0:30	23,510	1935k	7,292	637k	16,218	1298k
fe80::c30c:0:0:31	18,326	1494k	10,994	916k	7,332	577k
fe80::c30c:0:0:32	6,251	531k	5,719	480k	532	51k
fe80::c30c:0:0:33	72,301	4872k	58,254	3739k	14,047	1132k

Figure 10. Analysis of Traffic Generated by Motes in IoT Network

As shown in Figure 10, the node with fe80::c30c:0:0:33 IPV6 address has created much more packet traffic than other nodes. In a normal DODAG network, the most packet traffic should be at the mote farthest from the root mote (with the most Parent/Child relationships) and should show a steady increase in traffic. However, in the attack scenario, the attacking mote sent approximately two times more packets than the farthest mote, and a serious irregularity also has been detected in traffic increases.

The outlier feature has been used in the machine learning analysis of the study. This is because the attacker sends a large amount of HELLO packets in the flood attack, even if it is from inside or outside. In this context, the standard messaging between the motes will be out of the way and will come to the outlier position. This will allow the attacker to be detected early, taken out of the system, or blocked by security systems. In the flood attack, the K-Means algorithm, which considers the outlier features, is used because the attacker is far away from the average value of the network traffic. K-means algorithm is generally the most known and used clustering method. There are various extensions of the k-means to be proposed in the literature. Although there is unsupervised learning for clustering in pattern recognition and machine learning, the k-means algorithm and its extensions are always affected by initializations with the required number of clusters. That is, the K-means algorithm is not exactly an unsupervised clustering method [23]. The K-means algorithm is an algorithm for placing N data points in a set K in an I-dimensional space. Each cluster is parameterized with a vector m(k), called its mean. Data points will be denoted by {x(n)} where the superscript n runs from 1 to the number of data points N. Every x vector has an I component. Let's assume that the space x lives in is a real space and we have a metric that describes the distances between points, for example,

Given the first set of k-means m1(1),...,mk(1), the algorithm alternates between two steps:

Assignment step: Assign each observation to the cluster with the closest Euclidean mean. Each xp is assigned exactly one S(t), even if it can be assigned to two or more.

Update step: Recalculate the means (centers) for the observations assigned to each cluster.

The algorithm converges when the assignments no longer change. The algorithm is not guaranteed to find the optimum. The algorithm is usually presented as assigning objects to the nearest cluster based on distance. Using a distance function other than the (squared) Euclidean distance may prevent the algorithm from converging. Various modifications of k-means, such as spherical K-means and K-medoids, have been proposed to allow the use of other distance measures [24]. By using K-means algorithm, the anomaly mote (attacker mote) on the network traffic has been detected, as seen in Figure 11.

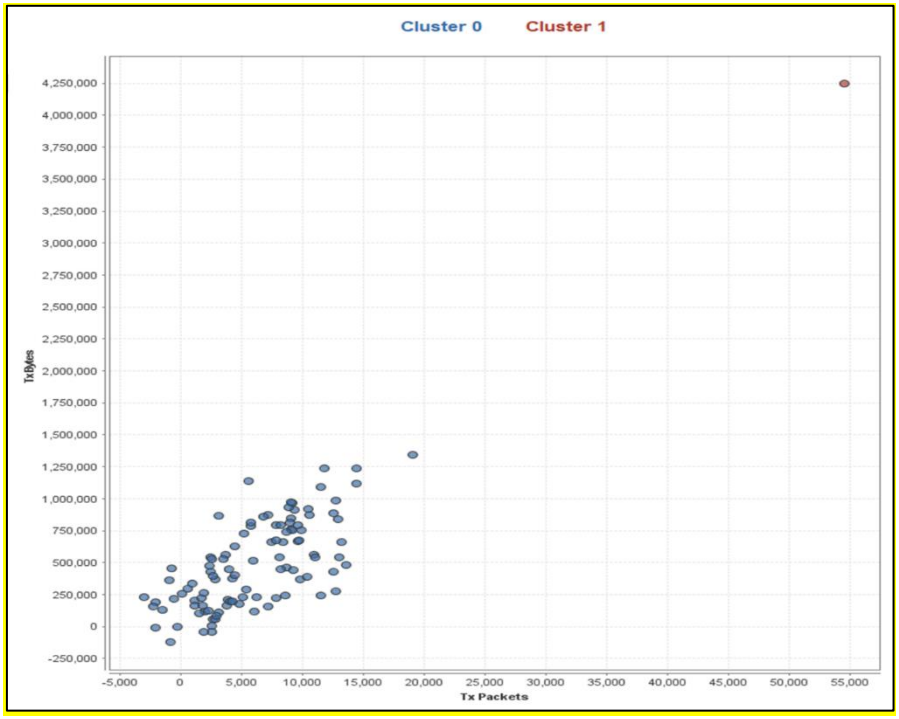


Figure 11. Analysis of the Nodes after the Application of the K-Means Algorithm

As seen in Figure 11, two different clusters were created as a result of machine learning. From these clusters, cluster-0 represents normal network traffic motes, and cluster-1 represents offensive mote. Due to a very extreme anomaly, the clusters in question are located at opposite points on the Plot axis.
The algorithm for the study is given below.

Input: IoT Dataset
Output: Attack or Legal Transmision
1: Load attributes of the dataset
2: *[rank,weights]=relief(features,target);* // Apply relief to calculate features ranks and means
2: **for** i = 1 to 7 **do**
3: *features outliner(:,I) = features (:,rank(I));* //Select outliner features.
4: **end for i**
5: acc^{mean} = 0; // Define accuracy value
5: **while** data(i)=outliner(i) do
6: attack=attack+1

7: acc = 0;
8: **for** i = 1 to L **do** // L is data set
9: **if** outliner(i) = flagedattack(i) **then**
10: acc = acc + 1;
11: **end if**
12: **end for i**
13: $acc^{mean} = acc^{mean} + \frac{acc}{L}$;
14: **end for j**

6. Discussion

In the study, the targeted aim of attack detection with hello flood attack analysis and artificial intelligence system has been achieved. During the study, completely original packages have been used and simulations have been carried out on these packages. During the simulations, both the instantaneous effect on the system and the effect on the system after the attack have been examined. As a result of the Hello Flood attack, it has been observed that power consumption on IoT devices have increased and network communication has been blocked. For these reasons, it is shown that a critically important system in which a hello flood attack can be carried out can cause very bad results. During artificial intelligence monitoring, this attack has been successfully detected with the K Means algorithm. This has proven how important it is to have an artificial intelligence system-supported IDS, which constantly monitors the network and monitors the packet traffic, waiting for a possible attack. This add-on ensures both the integrity of the system and the operation of the system in appropriate conditions. In the results of the analysis, an artificial intelligence system supported IDS is presented as a measure for network protection in order to protect it from attacks aimed at blocking IoT network communication.

7. Conclusion

With the developments in information technologies, every area of our lives, from shopping to education, from health to entertainment, has transitioned to the cyber environment, which is defined as the digital environment. In particular, the advances in short distance low energy communication platforms and embedded system technologies have included the concept of IoT, which enables many applications for the benefit of humanity. With the IoT process, unimaginable possibilities have been put at the service of humanity. However, the security dimension, which is not sufficiently taken into account and/or not included in this process, has also led to the emergence of important threats. The addition of IoT-specific vulnerabilities to existing vulnerabilities has led to the underutilization of the potential of IoT.

In this study, the Flood attack, which is one of the important attacks against IoT, is discussed. Within the scope of the analysis of the study, considering a fixed WSN, temperature, humidity, pressure, etc. a flood attack has been carried out by adding an offensive IoT mode to the reference network where the central IoT node is located, which collects IoT devices and values from these devices and transmits them to the relevant official. Changes in the IoT network during the attack and its effects on the system have been examined in terms of power consumption and changes in network traffic packets, which are the most important constraints of IoT networks. The results obtained at this stage have been explained that the attacker creates a significant load on the network traffic and the power consumption has increased considerably, and that there will be important material and moral consequences as a result of the attack. In the second stage of the analysis, the logs obtained on the reference and attacker network were analyzed with machine learning algorithm.

In this study, the effect of the flood attack on the IoT network on the system, attack analysis, and machine learning algorithm detection are focused. In the next study, other types of attacks against the IoT network will be analyzed.

Authors' contributions

All authors participated equally. Each author has worked at every stage.

Both authors read and approved the final manuscript.

Competing interests

The authors declare that they have no competing interests.

Refereneces

[1]. Lin, H., Bergmann, N. W., IoT privacy and security challenges for smart home environments. Information, 2016, 7(3), 44.
[2]. Nawaratne, R., Alahakoon, D., De Silva, D., Chhetri, P., Chilamkurti, N., Self-evolving intelligent algorithms for facilitating data interoperability in IoT environments. Future Generation Computer Systems, 2018, 86, 421-432.
[3]. Chouhan, P. K., McClean, S., Shackleton, M., Situation assessment to secure IoT applications. In 2018 Fifth International Conference on Internet of Things: Systems, Management and Security, 2018, pp. 70-77, IEEE.
[4]. Ravi, N., Shalinie, S. M., Learning-driven detection and mitigation of DDoS attack in IoT via SDN-cloud architecture. IEEE Internet of Things Journal, 2020, 7(4), 3559-3570.
[5]. Firouzi, F., Farahani, B., Weinberger, M., DePace, G., & Aliee, F. S., IoT fundamentals: definitions, architectures, challenges, and promises. In Intelligent internet of things 2020, pp. 3-50, Springer, Cham.
[6]. Niraja, K. S., & Rao, S. S., A hybrid algorithm design for near real time detection cyber attacks from compromised devices to enhance IoT security. Materials Today: Proceedings, 2021
[7]. Syed, N. F., Baig, Z., Ibrahim, A., & Valli, C., Denial of service attack detection through machine learning for the IoT. Journal of Information and Telecommunication, 2020, 4(4), 482-503.
[8]. Ahmad, R., & Alsmadi, I., Machine learning approaches to IoT security: A systematic literature review. Internet of Things, 2021, 14.
[9]. Lin, T., Deep Learning for IoT. In 2020 IEEE 39th International Performance Computing and Communications Conference (IPCCC), 2020, pp. 1-4, IEEE.
[10]. Tyagi, H., Kumar, R., Attack and Anomaly Detection in IoT Networks Using Supervised Machine Learning Approaches. Rev. d'Intelligence Artif., 2021, 35(1), 11-21.
[11]. Xiao, L., Wan, X., Lu, X., Zhang, Y., Wu, D., IoT security techniques based on machine learning: how do IoT devices use AI to enhance security? IEEE Signal Process, 2018, Mag. 35 (5), 41–49
[12]. Stellios, I., Kotzanikolaou, P., Grigoriadis, C., Assessing IoT enabled cyber-physical attack paths against critical systems. Computers & Security, 2021,107, 102316.
[13]. Yazdinejadna, A., Parizi, R. M., Dehghantanha, A., Karimipour, H., Federated learning for drone authentication. Ad Hoc Networks, 2021, 102574.
[14]. Mandal, K., Rajkumar, M., Ezhumalai, P., Jayakumar, D., Yuvarani, R., Improved security using machine learning for IoT intrusion detection system. Materials Today: Proceedings, 2020.

[15]. Singh, R., Singh, J., Singh, R., Fuzzy based advanced hybrid intrusion detection system to detect malicious nodes in wireless sensor networks. Wireless Communications and Mobile Computing, 2017.
[16]. Cakir, S., Toklu, S., Yalcin, N., RPL Attack Detection and Prevention in the Internet of Things Networks Using a GRU Based Deep Learning. IEEE Access, 2020, 8, 183678-183689.
[17]. Ioulianou, P., Vasilakis, V., Moscholios, I., Logothetis, M., A signature-based intrusion detection system for the Internet of Things. Information and Communication Technology Form, 2018.
[18]. Raza, S., Wallgren, L., Voigt, T., SVELTE: Real-time intrusion detection in the Internet of Things. Ad hoc networks, 2013, 11(8), 2661-2674.
[19]. Shreenivas, D., Raza, S., Voigt, T., Intrusion detection in the RPL-connected 6LoWPAN networks. In Proceedings of the 3rd ACM international workshop on IoT privacy, trust, and security, 2017, 31-38.
[20]. Napiah, M. N., Idris, M. Y. I. B., Ramli, R., Ahmedy, I., Compression header analyzer intrusion detection system (CHA-IDS) for 6LoWPAN communication protocol. IEEE Access, 2018, 6, 16623-16638.
[21]. Yavuz, F. Y., Devrim, Ü. N. A. L., Ensar, G. Ü. L., Deep learning for detection of routing attacks in the Internet of things. International Journal of Computational Intelligence Systems, 2018, 12(1), 39-58.
[22]. Jan, S. U., Ahmed, S., Shakhov, V., & Koo, I., Toward a lightweight intrusion detection system for the Internet of things. IEEE Access, 2019, 7, 42450-42471.
[23]. MacKay, David, "Chapter 20. An Example Inference Task: Clustering" (PDF). Information Theory, Inference and Learning Algorithms. Cambridge University Press, 2003, 284–292.
[24]. Sinaga, K. P., & Yang, M. S., Unsupervised K-means clustering algorithm. *IEEE access*, *8*, 2020, 80716-80727.