Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 45 No. 2 (2024)

Cross Layer Based DDoS Attack Detection in Internet of Things Using Machine Learning Algorithms

K. Saranya[1] and Dr.A. Valarmathi[2]

[1]*Full - Time Research Scholar, Faculty of Information and Communication Engineering, UCE-BIT Campus, Tiruchirappalli, Anna University, Chennai, Tamilnadu, India.*

[2]*Assistant Professor, Department of Computer Applications, UCE-BIT Campus, Tiruchirappalli, Anna University, Chennai, Tamilnadu, India*

Abstract:- A cross-layer approach is an effective and practical security defense mechanism. To prevent unauthorized access, multiple intruders causing abnormal traffic to the server cause DDoS attacks. The DNS flood denotes DDoS attacks in which an intruder floods specific domain in the DNS server. DNS flood attacks will compromise the website with network traffic that distinguishes heavy traffic. In this approach, it focuses on a cross-layer intrusion detection system that specifically detects DDoS attacks from the transport layer and network layer. To detect DDoS attacks like TCP SYN flood, UDP flooding attack and ICMP flood at the corresponding layers of the IoT are analyzed using a machine learning-based algorithm. In the transport layer, TCP SYN floods with synchronization flooding and UDP floods where the attacker overwhelms the random ports on hosts with IP packets in the network layer, it focuses on ICMP flooding, where the attacker overwhelms those targeted devices with ICMP echo requests (also called ping requests). We also used many machine learning algorithms such as Decision tree, KNN, MLP and Logistic Regression to detect abnormal activities such as DDOS features. In the experimental results, we found that the KNN and decision tree achieved high accuracy to detect attacks.

Keywords*:* Cross-Layer Security, DDoS attacks, IoT, Network Layer, Transport Layer.

1. Introduction

Cross-layer security indicates that devices with actuators and sensors that collect data are communicated through a wired or wireless medium in a secured manner. IoT devices, such as personal devices, are linked via a network, which must be secured. Since the devices are connected via a network, the data can be accessed anywhere. Cross-layer security allows information sharing where the layers tend to reduce overhead. Cross-layer security is designed to analyse the overall health condition of the device. Since IoT devices are connected via the internet, their data security is at great risk. One of the primary goals is to ensure that data is collected and transferred via network medium. as the IoT devices interact with different devices in heterogeneous environments. Sensors incorporated with the IoT devices are in different parts of the world. The data transmission tends to have a high rate of distortion, which is relatively unreliable. To enhance the overall performance, QoS with IoT improves the layering approach within the architecture. Cross-layer security tends to be highly adaptive, which transfers multimedia resources. The hiding of information primarily on wireless ad-hoc networks uses encapsulation. The layered architecture adjoins the data, which it processes and delivers whether data is received at the end or not. Cross-layer security communicates with other layers by increasing transparency and decreasing latency. By exchanging large amounts of data, it can improve the QoS where the sensors gather.

Cross-layer design enables data sharing among each layer, which is effective for IoT devices. Protocols are implemented by enabling a better encryption standard on IoT devices. IoT devices work with various environments, which connect with a plethora of heterogeneous devices with a diverse range of APIs. The primary functions of IoT devices are focused on various interoperability where it follows cross-platform operability. Cross-platform operability can access the different IoT platforms, which combine the different inputs from different applications. IoT application developers use this profound knowledge to build platform-specific APIs, which require tools to build their applications. Cross-layer design shares information where those layers make efficient

use of those network resources, which achieves high adaptivity. This layer is characterised by a few parameters that determine the best adaptation rules. It resolves the optimization issues with variables and constraints. The optimization space in wireless networks allocates the necessary aspects with multiple layers to make the best use of limited resources. The development of interoperable systems is aided by the use of standard layered protocols. The wireless connection between two nodes is determined by the distance between the distant locations. The physical medium handles several performances, such as limited bandwidth, propagation, and severe interferences. Optimization requires the information exchange between two or more layers of that protocol stack. TCP/IP coexistence and interoperability are examples of cross-layer solutions.

2. Literature Review

(Khakwal 2022) considers that security is the major concern of the IoT (Internet of Things). The diverse set of devices is specified with resource constraints, and the DoS attacks are frequent attacks where the attacks ensure multiple layers are compromised. In this study approach, a cross-layer intrusion detection system detects multiple DoS attacks on multiple devices. Different attacks are proposed to detect such attacks, where the attacks are simulated on NetSim with an overall detection probability. (Rehman 2022) indicates the physical layer security within wireless sensor networks, where it is used in civil and military fields. Information within wireless mediums transmits wirelessly, where the security of wireless sensor networks plays a major role. To address the critical issues identified across the various parameters of the security design model, various techniques are employed. Major attacks such as the TCP/IP model and its mitigation techniques are analyzed. The proposed methodology enhances the security of the WSN using the alpha and handshake techniques. (ZALP 2022) indicates the Internet of Things in smart devices where the devices are used in smart cities, public transport, and smart grids. The Internet of Things (IoT) devices connect the computer network. This method focuses on IoT devices within layer architecture, with the OSI layer being examined. Different potential vulnerabilities and attacks within IoT devices are investigated, and the IoT attacks are evenly classified. The common phenomena that enable those objects are various (Lalit 2022) communication technologies. Intelligent objects that are allowed to work autonomously through the internet IoT has diverse applications for transferring the data among those objects securely. The purpose of this paper is to discuss the various security protocols of application security protocols with various attacks and the consequences that the application may suffer as a result. (Saran, 2022) a number of cross-layer approaches based on machine learning techniques that have been offered in the past to address issues and challenges brought on by the variety of IoT are in-depth examined.

(Mishra, 2021) increase in significant risks due to security gaps, making users sceptical of IoT devices. IoT devices are vulnerable to security attacks, which cause financial and reputational losses. A multi-layered survey of various security issues within IoT systems within different layers of the model. Different DDoS attacks impact IoT devices and also provide solutions for mitigation. The review focuses primarily on IDS/IPS for mitigating DDoS attacks that trigger anomaly detection. Different IDS datasets with various ML and DL using pre-processed data have been reviewed. (Kore 2020) denotes the advancement of the Internet of Things, which uses wireless communication to monitor real-time applications. Secure data transmission with privacy enables the WSN's communications. Heterogeneity attacks, such as MAN, are currently used to layer security solutions. In this research, the cross-layer MAN system, which uses the robust clustering mechanism to form those clusters with cluster head preferences, is examined. The trust value is computed with various parameters that protect network communication in the presence of those security threats. (Abbas 2020) denotes the industrial IoT, which 5273tilized5273iz in the IoT that interconnects the industrial devices with control and intelligent processing devices to improve the industrial system's productivity. Heterogeneous industrial IoT devices collaborate with networks. The complexity of IoT systems is increased by cross-linking with a 5273tilized5273ized approach. In some of the literature, the evaluation of the experimental results is not guided. In this research, the multi-layer taxonomy of the IoT helps in understanding the incident attack pattern that impacts the industrial system. Taxonomy characteristics analyse the attack sequences, which envisage an efficient use of security platforms.

3. Proposed Methods

3.1. Transport layer Attacks

Layer 4 transport is the common protocol for transport, which exploits the normal TCP three-way handshake and sends the spoof attack through the targeted victim. A SYN flood attack targets the systems that are connected to

the internet and the transmission control protocol that attempts to forge the connection state. DdoS attacks target capable devices in networks with millions of connected devices. The offender sends through a TCP connection, where requests are processed faster than normal. Attacks use the repeated client to sync the packets to compromise the server using the rogue IP address, which causes the connection to be compromised. A SYN attack is a common type of DDoS attack that targets TCP connection sequences by sending the request via SYN, which sends the request via the open network connection between the client and the target server. The server receives the SYN request, which correspondingly responds to acknowledge the request by holding the connection open, and it waits until the client acknowledges the connection. SYN attacks occur when the attacker sends TCP to the target host to synchronise requests. TCP SYN attacks requests to those target hosts where the server is unavailable for the legitimate users. The transport layer describes the end-to-end message transfer capability that is independent of primary networks and consists of error control, fragmentation, and network flow control. In this layer, it reliably exchanges the data between two different endpoints. Some of the common types of TCP attacks are session hijacking, SYN flooding, and SSL malfunction.

The TCP/IP protocol exposes various attacks, which range from password sniffing to denial of service. TCP attacks, also known as SYN Flooding attacks, occur when a malicious host exploits the small size of the listened queue by sending multiple SYN requests, but the SYN-ACK response never arrives. Attackers replicate the packets that are being sent through the communication path. Threats at the transport layer aim to compromise the protocols utilized in order to deliver network connectivity among multiple devices. Such assaults have the ability to obstruct, interrupt, or alter data transmission among two destinations. Such assaults are frequently used to obtain private data or restrict the use of assets or operations. Assaults on the TCP protocol can frequently be hard to spot and have negative effects. To obtain information or interrupt operations, intruders may employ a number of strategies, such as spoofing, man-in-the-middle attacks, and attacks involving denial of service.

In the case of the TCP SYN FLOOD attack, as shown in Figure 1, the attackers make use of forged IP addresses and send frequent SYN packets to all ports on a server. The server attempts to create a connection for these many requests with an SYN ACK packet. The server under attack waits occasionally for acknowledgment of the SYN ACK packet. Hereafter the server will not be able to close this connection and it stays open. This increasingly leads to a huge number of half-open connections and hence these attacks are also known as “half-open” attacks.

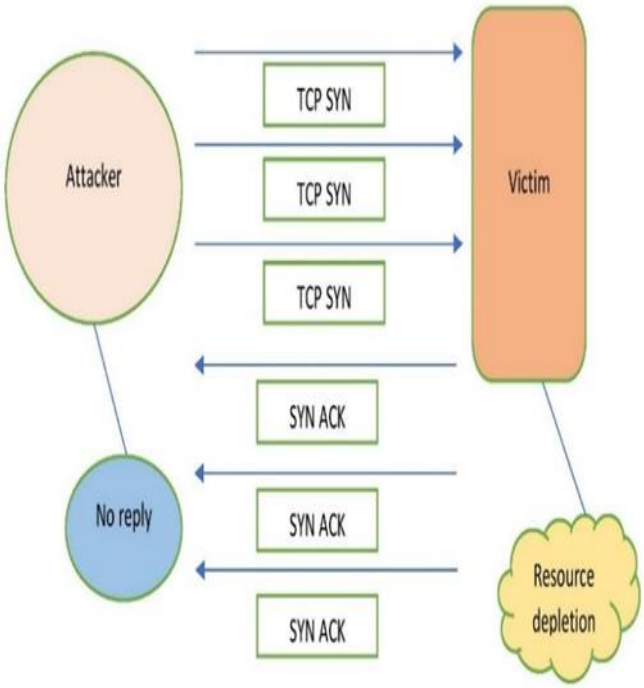


Figure 1. TCP SYN Flood Attack

3.1.1. TCP Flood Attacks

Transport layer, also called "ping flood," is a denial of service (DoS) attack where the attacker sends the victim a huge number of ping requests. Hence, the victim responds to those ICMP echo requests by sending a ping reply. The process is repeated until the victim is blocked by responding with a ping request and its responses. Ping flood attacks are considered the oldest attacks within networks because they Figure 2. Condition State of TCP Flood Attacks require high bandwidth, which saturates the networks with multiple ping requests. A TCP SYN flood attack might spoof the IP address in the ACK response, where the attack occurs when the malicious sender spoofs the ACK response. An ACK response spoofing, where the receiver never receives the complete TCP handshake. A typical connection request occurs between a legitimate client and server, where the client requests the connection by sending those SYN packets to the server. This server acknowledges requests by sending the SYN ACK packet to the client. The ACK message from the client side is established. Client requests connectivity by sending the TCP SYN message to the server. The server acknowledges by sending the connectivity to SYN ACK. SYN ACK acknowledge and sends back the message back to the client. Client replies with an ACK message where the connection gets established. Figure 2 illustrate the condition state of TCP flood attacks.

duration	protocol_type	service	flag	src_bytes	dst_bytes	land	wrong_fragment	urgent	hot	num_failed_logins	...	dst_host_srv_count	dst_host_same_srv_
0	tcp	http	SF	181	5450	0	0	0	0	0	...	9	
0	tcp	http	SF	239	486	0	0	0	0	0	...	19	
0	tcp	http	SF	235	1337	0	0	0	0	0	...	29	
0	tcp	http	SF	219	1337	0	0	0	0	0	...	39	
0	tcp	http	SF	217	2032	0	0	0	0	0	...	49	

5 rows × 41 columns

Figure 2. Condition State of TCP Flood Attacks

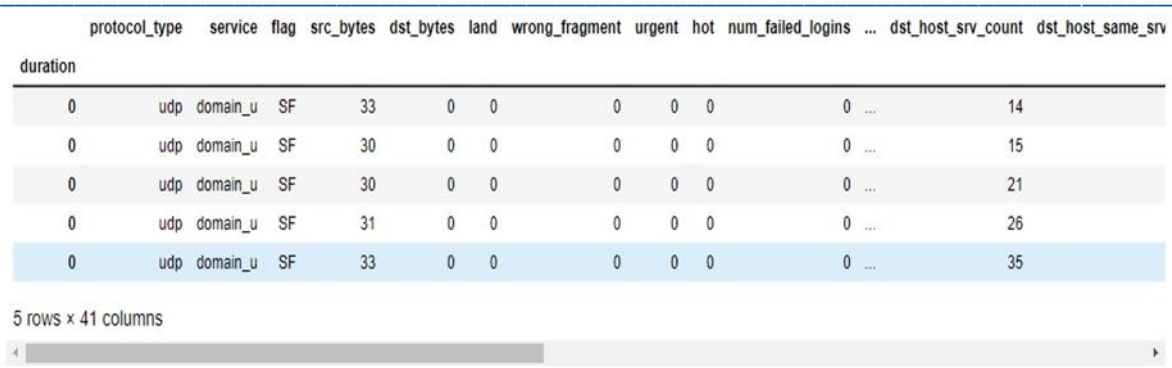
The following prototype with conditional statement of the TCP protocol indicates as follows:

```
tcp_syn_df = df[df.loc[:,"protocol_type"] == "tcp"]

tcp_syn_df = tcp_syn_df[tcp_syn_df.loc[:,"srv_serror_rate"] > 0.7]
```

3.1.2. UDP Flood Attacks

A UDP flood attack happens when an attacker sends a UDP packet to a random port on the victim's system, where the UDP packet determines what request is waiting on the port. It will create an ICMP packet for the destination, which will forge the source address. The system proceeds to the point where UDP packets deliver the ports on the targeted victim. large amount of UDP traffic with a spoofed IP address and random ports over the targeted system. Targeted servers are incoming packets within the listening host. When the number of packets received by the server becomes too large to handle, the system becomes overwhelmed and is unable to serve legitimate clients and users' requests. UDP packets are sent to the targeted server, where the device has a certain ability to respond. The connectionless protocol achieves no connection by establishing a connection between the client and server prior to packet transmission. An attacker sends that huge number of fake UDP packets to the target device. The UDP protocol within the transport layer gets attacked through flooding attacks. The attacker spoofs the IP address of those legitimate devices to hide his overall identity. Due to high packet counts, the attacker tries to send the victim's IP address to a random or specified port. Analyze the UDP request and determine the responses. The attacker sends the UDP packets to the victim, where they deplete the network bandwidth and also degrade the system. Figure 3 illustrate the condition state of UDP flood attacks.



duration	protocol_type	service	flag	src_bytes	dst_bytes	land	wrong_fragment	urgent	hot	num_failed_logins	...	dst_host_srv_count	dst_host_same_srv
0	udp	domain_u	SF	33	0	0	0	0	0	0	...	14	
0	udp	domain_u	SF	30	0	0	0	0	0	0	...	15	
0	udp	domain_u	SF	30	0	0	0	0	0	0	...	21	
0	udp	domain_u	SF	31	0	0	0	0	0	0	...	26	
0	udp	domain_u	SF	33	0	0	0	0	0	0	...	35	

5 rows × 41 columns

Figure 3. Condition State of UDP Flood Attacks

The following prototype with conditional statement of the UDP protocol indicates as follows:

udp_df = df[df.loc[:,"protocol_type"] == "udp"]

udp_df = udp_df[udp_df.loc[:,"srv_serror_rate"] > 0.7]

3.2. Network layer Attacks

The network layer exploits the common protocol for routing on the network. The network protocol collects the network stream of IP packets addressed to the network. The attacker uses routing protocols to absorb network traffic from source to destination, which regulates the abnormal network traffic flow. An attacker creates those routing loops, causing severe network congestion and channel contention. Network-layer networks are especially vulnerable to several DDoS attacks with different risks such as ICMP attacks, ping floods, smurf attacks, and IP spoofing. A network attack attempts to gain unauthorised access to an organization's network, which steals the data. Network attacks aim to breach the corporate network perimeter and gain access to internal systems.

Network security attacks divide a network into zones where subnets within the same zone are affected. Network-layer assaults are deliberate attempts to prevent computer networks from operating normally. Such attacks target the network layer of the OSI model, which is in charge of distributing data across various network nodes. Threats at the network level may result in major effects, including data loss, financial loss, and service interruption. A denial of service can also arise from DoS and DDoS attacks that make a system unresponsive. Attacks on the network layer can also be used to gain access to systems and take control of them. Attacks at the network layer may result in major effects, including loss of data, economic damage, and service interruption.

3.2.1. ICMP Flood Attacks

An ICMP flood targets the host with a large number of ICMP packets, which consumes a lot of bandwidth and denies legitimate access. A large number of sources send through the ICMP traffic, where the attacker floods the recipient device, which overwhelms the ICMP echo requests (ping flood). Within the target device, ICMP ping requests target the volume with rate limits. In this attack, it requires a valid IP address to target the internet layer protocol within network devices, which is diagnosed by analysing the ICMP echo-request and echo-reply messages. Attackers could spoof the bogus ip address to mask the sending device and sends the ICMP echo request packets within multiple devices. ICMP pings determines too many resources which renders the device unable to function. ICMP redirects the packets to the victim, which imitates the optimal gateway where the victim re-routes the traffic through the attacker, which allows the attacker to sniff. IP and MAC address sources are spoofs by the attacker. Figure 4 illustrate the condition state of ICMP flood attacks.

	protocol_type	service	flag	src_bytes	dst_bytes	land	wrong_fragment	urgent	hot	num_failed_logins	...	dst_host_srv_count	dst_host_same_srv_r
duration													
0	icmp	eco_i	SF	30	0	0	0	0	0	0	...	1	
0	icmp	eco_i	SF	30	0	0	0	0	0	0	...	11	
0	icmp	eco_i	SF	30	0	0	0	0	0	0	...	21	
0	icmp	eco_i	SF	30	0	0	0	0	0	0	...	31	
0	icmp	ecr_i	SF	30	0	0	0	0	0	0	...	5	

5 rows × 41 columns

Figure 4. Condition State of ICMP Flood Attacks

The following prototype with conditional statement of the ICMP protocol indicates as follows:

icmp_df = df[df.loc[:,"protocol_type"] == "icmp"]

icmp_df = icmp_dficmp_df.loc[:,"srv_serror_rate"] > 0.7]

4. Implementation

A combination of techniques called "cross-layer security" is employed to identify and stop harmful network traffic. To guard against hostile network connections, it uses numerous levels of protection, including firewalls, intrusion detection systems, and other security procedures. Cross-layer security can be used to recognize and stop malicious TCP flooding before it gets to the intended system. Although intrusion detection systems have the ability to find and stop malicious activity before it gets to the intended system, firewalls can find and stop anomalous activity. UDP flood defenses might be implemented using cross-layer security. Although intrusion detection systems are able to find and stop malicious activity before it gets to the intended system, firewalls can find and stop anomalous activity. In addition, network access control groups and rate limitation may be employed to restrict access to particular systems and services and the volume of traffic transmitted to the target network, respectively. The use of cross-layer security can effectively prevent hostile network activities. To guard against hostile network activity, it uses numerous levels of protection, including firewalls, intrusion detection systems, and other security measures. The use of cross-layer security can prevent TCP, UDP, and ICMP floods in addition to the detection and blocking of malicious traffic before it gets to the intended system. Cross-layer security is an idea that integrates the integrity of many system levels into a single, comprehensive security strategy. By establishing a comprehensive security environment, this strategy makes it possible to guard against hostile actors and flaws effectively. It entails the integration of security controls from several system levels, including the physical, network, and access layers. As a result, the system becomes more secured and therefore better capable of resisting intrusions and malicious actors. By merging many layers into a single system, it also lessens the complexities of security administration. Cross-layer security offers faster reaction times whenever a security breach is discovered by combining security protocols from many levels and improving insight into security occurrences.

5. Results Analysis

IoT systems with limited computing resources include a network layer in which communication plays a significant role, with various constraints such as communication range, network bandwidth, and power usage. These networking protocols are widely used in IoT, where they could fit in TCP/IP, which stacks appropriately. Users can access their IoT devices through multiple interfaces by analyzing network interface ports and web host ports. Security features are created to protect the firmware and applications operating on IoT devices, as well as their communications with users, the back-end infrastructure, and third-party applications at the device layer. In the IoT ecosystem, physical activities, including nanoscale probes and computer-aided manipulations that actively interfere with the hardware devices, can potentially result in security threats. Table 1 shows as the comparative analysis of all algorithms and Table 2 shows as the overall accuracy assessment analysis of TCP, UDP and ICMP flood attacks.

Table 1. Comparative Analysis

Logistic Regression	**precision**	**recall**	**f1-score**	**support**
0	0.00	0.00	0.00	9
1	1.00	1.00	1.00	26119
Accuracy			1.00	26128
macro avg	0.50	0.50	0.50	26128
weighted avg	1.00	1.00	1.00	26128
KNN				
0	1.00	1.00	1.00	9
1	1.00	1.00	1.00	26119
Accuracy			1.00	26128
macro avg	1.00	1.00	1.00	26128
weighted avg	1.00	1.00	1.00	26128
MLP Classifier				
0	0.00	0.00	0.00	9
1	1.00	1.00	1.00	26119
Accuracy			1.00	26128
macro avg	0.50	0.50	0.50	26128
weighted avg	1.00	1.00	1.00	26128
Decision Tree				
0	1.00	1.00	1.00	9
1	1.00	1.00	1.00	26119
Accuracy			1.00	26128
macro avg	1.00	1.00	1.00	26128
weighted avg	1.00	1.00	1.00	26128

Table 2. Overall Accuracy Assessment Analysis

Attacks	**Accuracy**	**Overall Accuracy**
TCP SYN Flood	99.9825	99.92
UDP Flood	99.905	
ICMP Flood	99.895	

Using the comparative analysis of ML algorithms such as logistic regression, KNN, MLP, and decision tree classifier, respectively, Protocol_type, service, flag, src_bytes, and des_bytes are used to differentiate between condition 1 and normal condition state 0. Based upon the accuracy classification algorithm, the decision tree (DT) gives the better performance in detecting the TCP-SYN flood attacks using cross-layer security mechanism to defend the overall security layers in IoT devices.

Figure 5 shows as the TCP SYN Flood, UDP Flood and ICMP Flood Attacks in Machine Learning Analysis of Logistic Regression, KNN, MLP and Decision Tree algorithms.

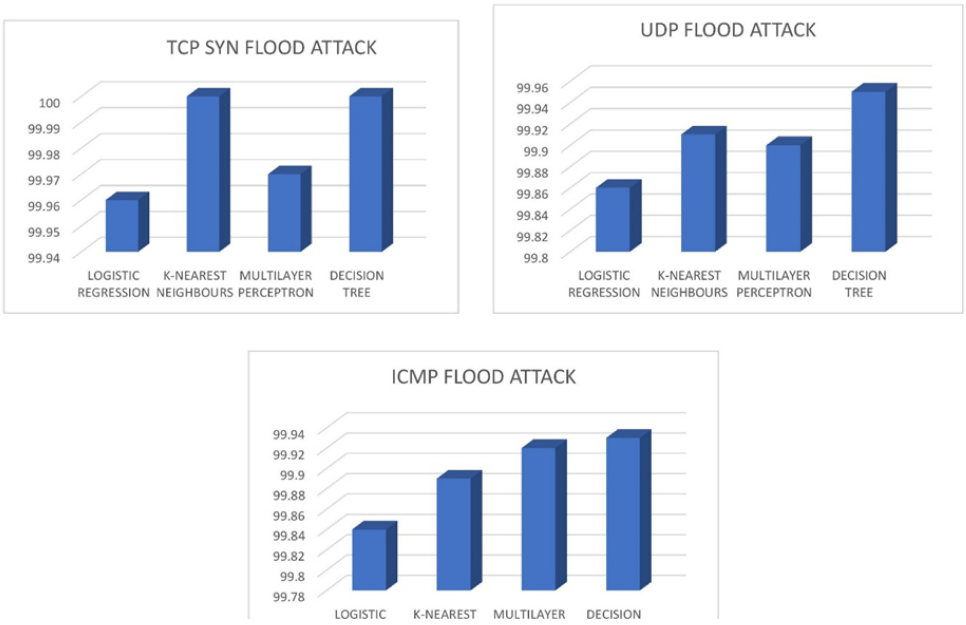


Figure 5. TCP SYN Flood, UDP Flood and ICMP Flood Attacks ML Analysis

6. Conclusion and Future Works

In order to identify DDoS attacks at the IoT layer, machine learning algorithms are used to assess TCP SYN flooding, UDP flooding attacks, and ICMP flooding. These analyses occur at the lower level of the network stack (layer 4), which is dependent on high volumes of traffic for normal operation. When bandwidth usage falls below a certain threshold, web server performance can be compromised. to enhance the security solution of the environment with a layered approach and defense mechanisms. Multiple intruders cause abnormal traffic to the server, which causes DDoS attacks. To effectively protect against DDoS attacks originating from the network and transport layers, a cross-layer intrusion detection system uses a machine learning algorithm to identify three separate types of attack: a TCP SYN flood, a UDP flooding attack, and an ICMP flood. Flooding attacks that use TCP SYN and UDP floods are employed at the transport layer. The attacker sends packets to random ports on the targeted device in an attempt to elicit a reaction from the target. This type of attack is focused specifically on ICMP flooding-offloading incidents (known as "ping" attacks) at the network level. Interspersed among these assaults are IP flooding attacks, which involve sending unlimited amounts of ICMP echo requests to a single host. We calculate the detection accuracy for each attack and show that as the accuracy increases considerably. In future we may incorporate more attacks and design a single NN to detect multiple cross layer DDoS attack simultaneously.

Refrences

[1] Kharkwal, S. Mishra and A. Paul, "Cross-Layer DoS Attack Detection Technique for Internet of Things," 2022 7th International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 2022, pp. 368-372, doi: 10.1109/ICCES54183.2022.9835924.

[2] Rehman, A.U. , Mahmood, M.S., Zafar, S., Raza, M.A., Qaswar, F., Aljameel, S.S., Khan, I.U., Aslam, N., A Survey on MAC-Based Physical Layer Security over Wireless Sensor Network. Electronics 2022, 11, 2529. https://doi.org/10.3390/electronics11162529

[3] A. N. ÖZALP, Z. ALBAYRAK, M. ÇAKMAK and E. ÖZDOĞAN, "Layer-based examination of cyber-attacks in IoT," 2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), Ankara, Turkey, 2022, pp. 1-10, doi: 10.1109/HORA55278.2022.9800047.
[4] M. Lalit, S. K. Chawla, A. K. Rana, K. Nisar, T. R. Soomro and M. A. Khan, "IoT Networks: Security Vulnerabilities of Application Layer Protocols," 2022 14th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS), Karachi, Pakistan, 2022, pp. 1-5, doi: 10.1109/MACS56771.2022.10022971.
[5] N. Mishra and S. Pandya, "Internet of Things Applications, Security Challenges, Attacks, Intrusion Detection, and Future Visions: A Systematic Review," in IEEE Access, vol. 9, pp. 59353-59377, 2021, doi: 10.1109/ACCESS.2021.3073408.
[6] K.Saranya, A.Valarmathi, "A Comparative study on Machine Learning based Cross Layer Security in Internet of Things (IoT)" , International Conference on Automation, Computing and Renewable Systems (ICACRS 2022) DVD Part Number: CFP22CB5-DVD: ISBN: 978-1-6654-6083-52022 .
[7] A. Kore and S. Patil, "Robust Cross-Layer Security Framework for Internet of Things Enabled Wireless Sensor Networks," 2020 International Conference on Emerging Smart Computing and Informatics (ESCI), Pune, India, 2020, pp. 142-147, doi: 10.1109/ESCI48226.2020.9167555.
[8] S. G. Abbas, F. Hashmat and G. A. Shah, "A Multi-layer Industrial-IoT Attack Taxonomy: Layers, Dimensions, Techniques and Application," 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Guangzhou, China, 2020, pp. 1820-1825, doi: 10.1109/TrustCom50675.2020.00249.
[9] R. H. Venkatnarayan, P. Adina, S. Mahmood and M. Shahzad, "Poster: A framework to secure IoT networks against network layer attacks," 2019 IFIP Networking Conference (IFIP Networking), Warsaw, Poland, 2019, pp. 1-2, doi: 10.23919/IFIPNetworking46909.2019.8999464.
[10] Y. Zhang, L. Duan, C. -A. Sun, B. Cheng and J. Chen, "A Cross-Layer Security Solution for Publish/Subscribe-Based IoT Services Communication Infrastructure," 2017 IEEE International Conference on Web Services (ICWS), Honolulu, HI, USA, 2017, pp. 580-587, doi: 10.1109/ICWS.2017.68.
[11] R. Sharma, N. Pandey and S. K. Khatri, "Analysis of IoT security at network layer," 2017 6th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, 2017, pp. 585-590, doi: 10.1109/ICRITO.2017.8342495.
[12] R. Song, H. Tang, P. C. Mason and Z. Wei, "Cross-Layer Security Management Framework for Mobile Tactical Networks," MILCOM 2013 - 2013 IEEE Military Communications Conference, San Diego, CA, USA, 2013, pp. 220-225, doi: 10.1109/MILCOM.2013.46.
[13] Wei, C., Li, Y., Lv, C. (2012). A Cross-Layer Security Framework for Wireless Mesh Networks. In: Zhang, Y. (eds) Future Wireless Networks and Information Systems. Lecture Notes in Electrical Engineering, vol 143. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-27323-0_14
[14] S. Nandi, "Network layer specific attacks and their detection mechanisms," 2011 2nd National Conference on Emerging Trends and Applications in Computer Science, Shillong, India, 2011, pp. 1-1, doi: 10.1109/NCETACS.2011.5751372.
[15] S. Ramachandran, G. Fairhurst, M. Luglio, C. Roseti and S. Provenzano, "Network Layer Security: Design for A Cross Layer Architecture," 2007 International Workshop on Satellite and Space Communications, Salzburg, Austria, 2007, pp. 271-275, doi: 10.1109/IWSSC.2007.4409429.
[16] Mingbo Xiao, Xudong Wang and Guangsong Yang, "Cross-Layer Design for the Security of Wireless Sensor Networks," 2006 6th World Congress on Intelligent Control and Automation, Dalian, 2006, pp. 104-108, doi: 10.1109/WCICA.2006.1712371.
[17] Ayushi Kharkwal, Saumya Mishra, Aditi Paul,Cross-Layer DoS Attack Detection Technique for Internet of Things, Proceedings of the Seventh International Conference on Communication and Electronics Systems (ICCES 2022) IEEE Xplore Part Number: CFP22AWO-ART; ISBN: 978-1-6654-9634-6, 2022.
[18] Amar Amouri, Vishwa T. Alaparthy and Salvatore D. Morgera, Cross layer-based intrusion detection based on network behavior for IoT in 2018.
[19] Vivek Kumar Asati, Emmanuel S. Pilli, S. K. Vipparthi, Shailesh Garg, Shubham Singhal, and Shubham Pancholi, RMDD: Cross Layer Attack in Internet of Things, in 2018.
[20] Sumathi, R.Rajesh, Comparative Study on TCP SYN Flood DDoS Attack Detection: A Machine Learning Algorithm Based Approach, WSEAS Transactions on Systems and Control in November 2021.
[21] R. Karimazad and A. Faraahi, An anomalybased method for DDOS attacks detection using rbf neural networks, in 2011 International Conference on Network and Electronics Engineering, IPCSIT, vol. 11, 2011.