IoT Networks: Using Machine Learning Algorithm for Service Denial Detection in Constrained Application Protocol

[1]Adamu Abdullahi, [2]O. N. Francisca, [1]Saidu Isah Rambo, [1]G. N. Obunadike, [1]D. T. Chinyio

[1]Department of computer science, Nigerian Defence Academy, Nigeria

[2]Department of Cyber Security, Nigerian Defence Academy, Nigeria

✉: adamspolo@gmail.com; adamspolo@nda.edu.ng

Received:05.05.2023 **Accepted**:06.07.2023 **Published**: 06.07.2023

Abstract:
The paper discusses the potential threat of Denial of Service (DoS) attacks in the Internet of Things (IoT) networks on constrained application protocols (CoAP). As billions of IoT devices are expected to be connected to the internet in the coming years, the security of these devices is vulnerable to attacks, disrupting their functioning. This research aims to tackle this issue by applying mixed methods of qualitative and quantitative for feature selection, extraction, and cluster algorithms to detect DoS attacks in the Constrained Application Protocol (CoAP) using the Machine Learning Algorithm (MLA). The main objective of the research is to enhance the security scheme for CoAP in the IoT environment by analyzing the nature of DoS attacks and identifying a new set of features for detecting them in the IoT network environment. The aim is to demonstrate the effectiveness of the MLA in detecting DoS attacks and compare it with conventional intrusion detection systems for securing the CoAP in the IoT environment. Findings The research identifies the appropriate node to detect DoS attacks in the IoT network environment and demonstrates how to detect the attacks through the MLA. The accuracy detection in both classification and network simulation environments shows that the k-means algorithm scored the highest percentage in the training and testing of the evaluation. The network simulation platform also achieved the highest percentage of 99.93% in overall accuracy. This work reviews conventional intrusion detection systems for securing the CoAP in the IoT environment. The DoS security issues associated with the CoAP are discussed.
Keywords: Algorithm, CoAP, DoS, IoT, Machine Learning

1. Introduction

The Internet of Things (IoT) is the consequence of flooding a huge amount of physical papers on the Internet on an incredible scale. These physical things incorporate temperature sensors, advanced mobile phones, cooling, therapeutic hardware, lights, brilliant frameworks, indoor regulators, and Televisions (TVs), but not restricted to them. In many research considerations, the significance of IoT frameworks in different parts of our lives has been explained in bringing organized knowledge to physical items around the world, enabling them to detect and collect natural information. IoT safety is the biggest concern for natives, clients, organizations, and governments that need to shield their products from hacking or negotiating, and should be targeted with alertness [1].

Constrained Application Protocol (CoAP) is a protocol for lightweight machine-to-machine (M2M) operating on smart devices where storage and recording resources are uncommon. DoS point of perspective, CoAP is a protocol that is performed for both Transmission Control Protocol (TCP) and User Datagram Protocol UDP and does not expect verification to respond with a huge response to a small request. More than 400,000 of the devices are being used in attacks, and the latest A10 Networks report discovered, that CoAP is a fundamental UDP convention for low-control PCs on questionable devices that looks like Hyper Text Transfer Protocol (HTTP) but operates over port 5683 of UDP [2].

Denial of Service (DoS) attack using CoAP begins with gadget inputs that can be managed and continue with a surge of parcels ridiculed with their goal's source address. These attacks concentrate on a broad range of resources at the application layer and can cut down a server much faster than system layer Distribution Denial of Services (DDoS) attacks, and with significantly more speed. In the (IoT), there are countless things connected through a scheme that can be sensors, actuators, or devices designed to collect data and transmit data [3].

[4-5] stated that these collected information reports are used to improve the execution of the scheme, improving the execution of products and administrations. It is estimated that up to 2022, a trillion physical goods will be connected to the Internet. This purpose could be met by the Interruption Detection System (IDS). DoS attacks can be aimed over each of the Transmission Control Protocol (TCP)/ Internet Protocol (IP) model layers.

Software-Defined Network (SDN) of IoT in CoAP is an emerging worldview scheme that has gained critical support from various experts in addressing the need for present server forms. CoAP uses DTLS to verify client-server correspondence as its safety convention, DTLS can't handle DoS attacks [6]. A Slow-Rate Application Layer DDoS attack misuses the ability of a server to trust associations will be completed promptly if the association approach is genuinely moderate [7-8].

The research aims to apply feature Selection and Extraction

algorithms to detect the DoS attack in CoAP using Machine Learning. The objectives are to analyze the nature of DoS attacks and the possibility of launching the DoS attacks in CoAP to identify a new set of features for detecting the DoS attacks using a machine learning algorithm in IoT Networks and provide a security scheme for CoAP against DoS attacks in the IoT environment using a machine learning algorithm.

2. Review of Related Literature

DoS attack is a significant risk to today's systems, Personal Computers (PCs), and correspondence frameworks. They have adversely affected associations, single customers, necessary Internet foundations, and so on, over the past decade or so DoS and DDoS is a serious effort to disturb, corrupt, or prevent authentic customers from accessing a data asset. DoS attacks (single and multiple sources) are straightforward to orchestrate and bring havoc to the target machine, the reason being the simplicity in design and user interface, without requiring any significant knowledge or expertise, or resources for their functioning. The attack tools are readily available on the Internet, especially in the Deep and Dark [9].

Jorge et al.[10], Setikere et al.[11], and Sicari et al.[12] study the impact of SD-Based instruction detection on DoS techniques and used experiments to unravel the negative of DoS in IoT sensor nodes and proposed an outline for IoT safeguard framework that can executive in various kinds of internet Protocol IP and Bluetooth DoS.

Sicari et al.[13] and Sun et al. [14] provide a response called REATO to efficiently and gradually identify and face DoS attacks within an operating IoT middleware. To approve the suggested approach, a real model has been recognized by assessing various relevant parameters. Security analysis and occasions enabled the control problem of the networked control system (NCSs) to detect DoS.

Gallais et al.[15] and Al-Hadhrami et al.[16] focused on connecting attacks that can be relieved by methodologies, such as time-division approaches and channel hopping. The designers use the IEEE 802.15.4e standard to show that methodologies such as these determine how to be resistant to sticking while remaining defenseless against particular sticking. Proposed an AI to recognize DoS in IoT devices and traffic from IoT scheme and break down traffic by going to attack location model for AI.

2.1 Modes of Operation of DOS in an IOT Network

This section reviewed the various modes of DoS operation attacks like UDP Flooding, ICMP Flooding, NTP Amplification, DNS Reflector Attack, and TCP-SYN Flooding Attacks.

2.1.1 UDP Flooding: Studies[17-18] proposed a new independent security framework, including structure, use, and experimental approval, to demonstrate the system's competent certainty against DDoS attacks by implementing countermeasures settled on and adopted by an autonomous framework rather than a human framework.

2.1.2ICMP flooding attack

ICMP convention provides us with a system administration component to check whether or not a remote PC is alive by sending an ICMP ECHO REQUEST bundle to the remote framework. If an ICMP flooding attack should occur, a huge amount of malignant ICMP ECHO REQUEST packages will be coordinated with the individual concerned.

2.1.3 Network Time Protocol Amplification

Since its presentation in 2012 (the number of assaults began in late 2013), DoS attacks using Network Time Protocol (NTP) enhancement are on the rise and dynamically more typical in recent memory than at any other time. The NTP Protocol is used for the synchronization of framework tickers and for the conveyance of the exact time on the web.

Studies [19-21] illustrated distinct processes and suggested distinct flood attack methods. The contribution of this study is that in MANETs, the authors have researched various flooding attacks and their identification methods with parameters of the execution measure. A decentralized security engineering based on SDN coupled with an IoT blockchain development arrangement in the wonderful town that relies on the three center developments of SDN, Blockchain, and Fog and mobile edge registration to acknowledge IoT attacks organize even more effectively.

2.1.4 Domain Name Server (DNS) Reflector Attack

Anagnostopoulos et al. [22] examine the ability of Top-Level Domain (TLD) and Authoritative Name Server (ANS) to be misused in Domain Name Server (DNS) intensification attacks as accidental carriers. The results findings are that 70% of the distinctive ANS and 47% of the conceivable DNS requests for the (TLDs) generate an enormous AF that exceeds 60, (ii) 10% of the specific ANSes reflect inbound system traffic and amplify it by a factor that exceeds 50, (iii) the amount of the most useful ANSes for the assailant, considering their work as enhancers, seems to be increasing.

Studies [23]-[24] conducted an estimate of the rate-restricting setups used by DNS servers for well-known spatial names, providing a better understanding of the precautionary measures taken to ensure the DNS foundation. Discovered a scheme by monitoring Domain Name Server Record Response (DNSRR) investigation traffic structuring the DNS traffic gathering action all the time sent by both devices. The investigation relies on the type of botnet attack, the target for recognition, including origin, emphasizes extraction, and includes connection, and AI strategies.

2.1.5 TCP-SYN flooding attack

Kak [25] Reviewed the IP and TCP packet headers, TCP Traffic Control and Shrew DoS Attack, TCP SYN Flood Attack for Denial of Service, IP Source Address Spoofing Attacks, and BCP 38 for Thwarting IP Address Spoofing for DoS Attacks,

Python and Perl Scripts for Mounting DoS Attacks with IP Address Spoofing and SYN Flooding and Troubleshooting Networks.

2.2 Internet of Things

IoT innovation against a few attacks is powerless. The increase in IoT of new correspondence conventions builds the probability of attacks. Denial-of-Service (DoS) attack is one of those attacks that have a critical concern on the Internet of Things. DoS attack's basic goal is to consume a server hub's resources and deny IoT authentic customers the services. A progression of huge DoS attacks against IoT gadgets was driven in 2016 and focused on the site of Brian Kreb. These hideous attacks feature the inclusion of approximately coupled security in IoT conventions, and security risks arise due to poor safety mechanisms over their devices.

Studies [26 - 27] present an attack recognition approach based on AI inconsistency identification procedures and a selection module to identify significant IoT attacks and further study focused on putting forward a model to check the IoT scheme as a keen home using a secured gateway device.

Authors [28-29] examined that the supply of the Internet of Things (IoT) devices could be depleted by a malevolent attacker by sending many wake-up radio (WUR) transmissions. Therefore, as required, strategies are given to empower an access point (AP) to identify any malicious WUR requirements. With station assistance (STAs), the AP can shrewdly relieve the attack. Suggested that IoT frameworks are observing boundless apps across countless undertakings and facing significant scalability and security challenges, such as transportation, utility, manufacturing, human services, home mechanization, etc.

[30] Investigated methods to prevent undermining and using IoT devices in a DDoS attack. The exploration's original part focused on what IoT devices are and their vulnerabilities. The following regions examined distinct types of attacks against IoT devices and several distinct methods of verifying the device. Different types of IoT operating frameworks were also discussed.

IoT devices with low computing power, [31] examined the feasibility of using a lightweight, low-rate DoS attack counterproductive action and control program. The objective is to empower these devices to prevent DoS attacks and regulate them.

Forchaos theory is developed in Andria by [32] for the smart home IoT network. As the stealth activities of DoS attacks, which is like seeming legitimate, it is difficult to differentiate the malicious activities from the legitimate nodes is difficult using intrusion detection systems. The For Chaos algorithm can identify legitimate and malicious activities by taking small training time and features. However, in some scenarios, the Forchaos results in false negatives.

[33] under the influence of internal and external nodes, a two-folded epidemic model is developed where an attack on IoT devices is first achieved, and then IoT based distributed attack of malicious objects on targeted resources in a network has been established. This model is mainly based on the Mirai botnet made of IoT devices which came into the limelight with three major

Hamdan [34] Presents a dual-mode IoT-based framework for screening and checking home devices. Home machines are interfaced with a widely helpful sophisticated and easy info and yield source of a lone chip microcontroller within the suggested framework.

Ullah [35] Conducted a study of IoT via PREVIEW devices working in industrial control systems and other critical infrastructure setups that can cause significant property loss and sometimes even livelihoods, a very sobering fact.

Silva [36] investigate the development of IoT framework and benefits from different scenarios obtained based on the software-defined network of IoT for the adaption of the technologies based on cloud and Edge Computing and security solution provides.

2.2.1 IOT Messaging Protocol

The heterogeneous and enormous amount of devices in the IoT causes a problem in monitoring the data trade between the devices, making the development framework for disruption (IDS) in IoT a future research problem. For example, a few conventions, (MQTT), (CoAP), Extensible Messaging and Presence Protocol (XMPP), and Advanced Message Queuing Protocol (AMQP) are familiar with exchanging the IoT message. MQTT is the best possibility for M2M correspondence in contrast to its partner, CoAP, because of its lightweight qualities and ability to work in low-control, restricted memory gadgets. The device detection begins to complete server communication through a gateway. Not all IoT devices are default verified and defenseless against different attacks [37].

Studies [38-39] observed and suggested that when forchaos provides high weight to tolerate unreliable communication while using DTLS, authentication, and authorization techniques based on the smart gateway to enhance DTLS transmits the sensitive data securely using Advanced Encryption Standard-Counter with Cipher Block Chaining-Message Authentication Code (AES-CCM) encryption and decryption algorithms and Stateful Protocol Analysis (SPA).

According to the following studies [40-41]. MQTT provides the least complicated and best data development by using distribution and purchase in the data stream for sensor arrangement. If this data is to be obtained outside the organization of the sensor, it should be accompanied by COAP for HTTP assistance. Highlighted the factors of low configurations of IoT devices protocol and countermeasures for an MQTT DoS attack is an SSL / TLS validation-dependent testament, which is not suitable for IoT devices since the managers expand the overhead computation and correspondence.

Dong et al.[42] extended the CoAP with a setting adjustment component to improve the assessment of the framework states and various assignments in the physical behavior demonstration and use protocol level.

Krawiec et al. [43] presented Dynamic Adaptive Streaming

over CoAP (DASCo), a response to the IoT condition of flexible media. DASCo consolidates DASH (Dynamic Adaptive Streaming over HTTP), the far-reaching open standard for HTTP-consistent spilling, with the CoAP (Constrained Application Protocol), and the free internet-moving protocol for resource-consuming devices.

Author [44] conducted a replica-based quantitative display evaluation of CoAP in HTTP examination, surveying the transmission of data depending on the main characteristics of dynamic system circumstances and expected situations.

Jarvinen et al. [45] Conducted a comprehensive scheme of analysis in different system environments and think about CoAP exhibition over TCP to the present CoAP over UDP clog control calculations. The results reveal that, despite the reality that CoAP over TCP has its known impediments, it scales well and works amazingly better than expected in certain distant environments for which CoAP over UDP calculations are explicitly designed, often notwithstanding the CoAP over UDP outflanking. However, both COAP and MQTT are intended for asset-based devices, supporting a wide range of customers including microchips, windows applications, and program-based applications.

In the report of the study[46] The creators affect the exceptional Californium CoAP code set up by the Eclipse Foundation, just as the U.S. Naval Research Laboratory's (NRL) Negative-Acknowledgment Oriented Reliable Multicast (NORM) code set proposes a reliable MANET transport agreement meaning CoAP over NORM (CoNORM).

According to the study[47], an enhancement of a CoAP protocol will be completed by focusing on the respectability message; designers will strive to identify the perfect hash function that can be added to the CoAP convention by extending the safety without influencing the exhibition. Using the Contiki OS recreation device on a passionate home implementation, the upgraded convention has been evaluated, and the results show that SHA 224 is the best hash calculation as per the lecture. Also, Hameed [48] discussed a requirement for remote detection and incitement, devices are continually integrated into the base of Internet correspondences, and the importance of recognizing and handling attacks against their security and stability is the main prerequisite.

Ioulianou et al. [49] described and discussed the Risks that can appear in the scheme (6LoWPAN) and application layers as (DoS) attacks and attacks by subverting CoAP use rules. IoT is a promising future worldview system that enables heterogeneous smart devices to correspond. The related amount of devices is expected to reach 50 billion by 2020.

According to Gohar [50], the study analyzed the existing scheme of CoAP Based IoT of proxy mobile internet protocol and investigate the IoT Devices in the new network access to the gateway for packet delivery through the NS-3 simulation to identify delays, packet losses for end-end, and throughput during the handover and compared the schemed.

Study [51] presented a model as an alternative to media transport in MQTT, RTP, and CoAP to determine the most efficient scenario for audio speech and video transmission. Identify the weakness of the traditional RTC protocol over Real Time Protocol for the context of Lower power lossy Networks.

Palmese et al. [52] investigated the protocol performance between MQTT-SN through the sensor network and CoAP in its version of publication and subscription. Both protocols were analyzed on UDP and transport layer for comparisons of the functionalities on the open sources platform. The comparison is based on theoretical and simulation environments and found that CoAP is the best choice for dynamic networks.

Bhatt and Ragiri [53] The authors investigate the pros and cons of the IoT data exchange protocol based on the vendor's policies and focus on the three features of performance known (jitter, latency, energy, and consumption) across different scenarios. The results obtained show that the CoAP was the best across all scenarios with the lowest time to compel while OPC and UA resulted in higher time completion in comparison to CoAP or MQTT.

3. Methodology

The research methodology is mixed-method, where datasets are generated from Social IoT and CIDDs, and real-time data on the IoT network environment is used to identify the research gap from the existing literature. The qualitative and quantitative methods are applied to enhance the security scheme for CoAP in the IoT environment.

Data Collection and Analysis Procedures, the data collection is done from Social IoT and CIDD, and real-time data on the IoT network environment is used for the research. The mixed-methods approach of qualitative and quantitative is used for feature selection, extraction, and cluster algorithms to detect DoS attacks in the CoAP. The k-means algorithm is used for training and testing the evaluation of the DoS attacks in the IoT network environment and compared with conventional intrusion detection systems.

The workflow methodology for Internet of Things Environment SIoTE is shown in Figure 1.

Figure 2 shows the data collection-flow process of the data collection methodology designed on real-time network sensors through the Contiki Cooja Network Platform and generated datasets from the three IoTdataset and traffic flaws repository on CIDDs, UNB, and SIoTE for detection of DoS attack using Machine Learning. Datasets are categorized into three different phases as shown in the diagram flow Data collection, Feature Selections and Extraction, and Machine Learning Classifier.

The steps in Figure 2 present a novel methodology applied in the implementation of DoS detection in an IoT Network Environment which described the processing stages and execution of the Machine Learning Algorithm in an IoTLAB testbed. The following processes described the classification algorithm of feature selection, Cluster Algorithm, and K-mean Cluster, used for the detection of DoS attacks in a CoAP. The collected overall datasets were trained and tested for the prediction of DoS attack accuracy. The following parameters used are Wrong URI, Wrong acknowledge, DoS Request, and DoS Acknowledge using machine learning algorithms.

3.1 Algorithm Classification

Based on datasets Extracted and selected for the processes a

total of 40,071,533 datasets, training, and testing then concatenating both using the Concat function. Evaluation of the generated classification algorithm to verify how valid the generated classification algorithms are and to compare the performance of the classification generated using the original dataset and the performance of the classification generated using the three algorithms dataset in training and testing ratio 10-folds cross-validation use in validating the performance of the model.

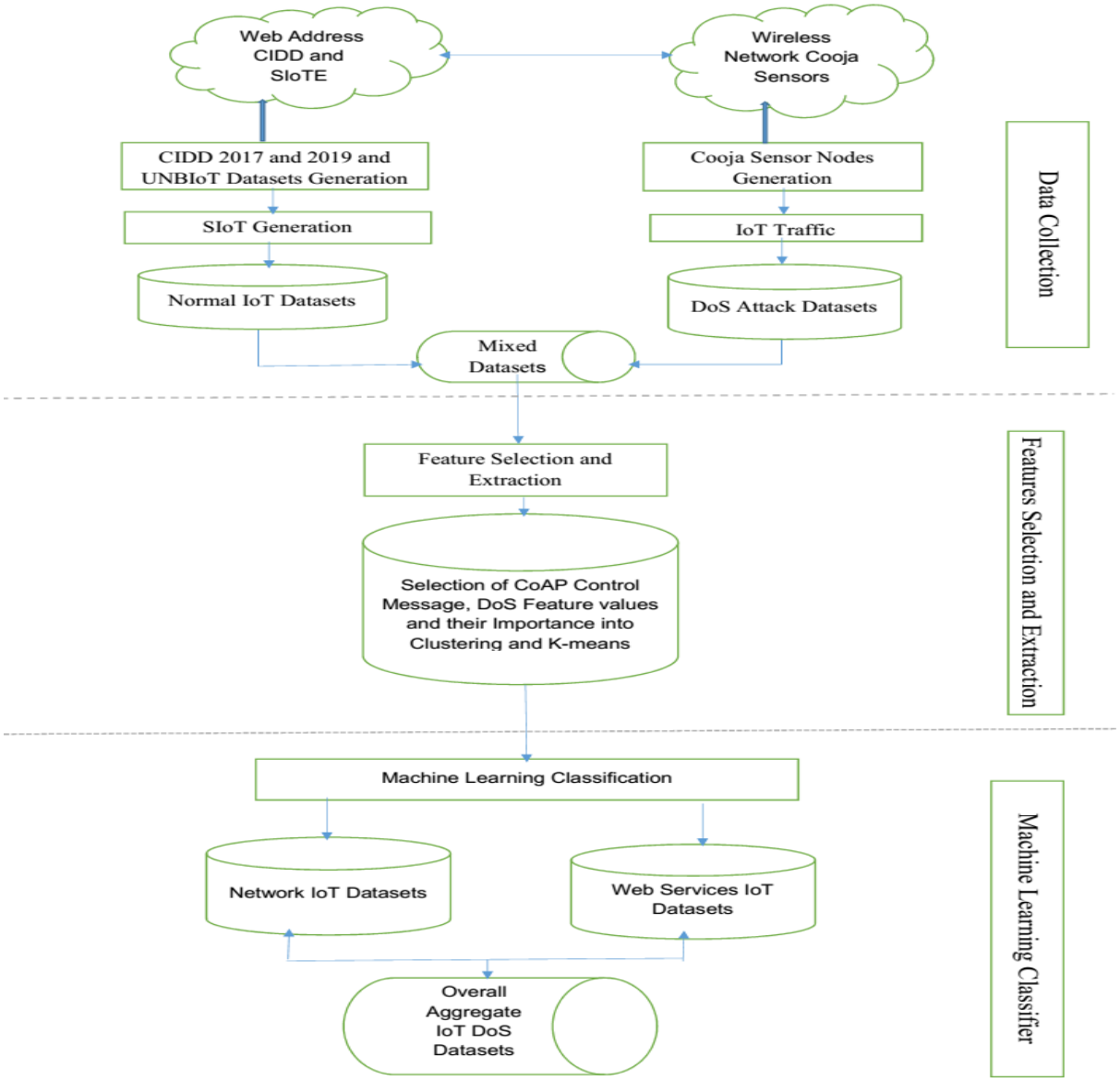

Figure 1. Methodology Designed for Data Collection.

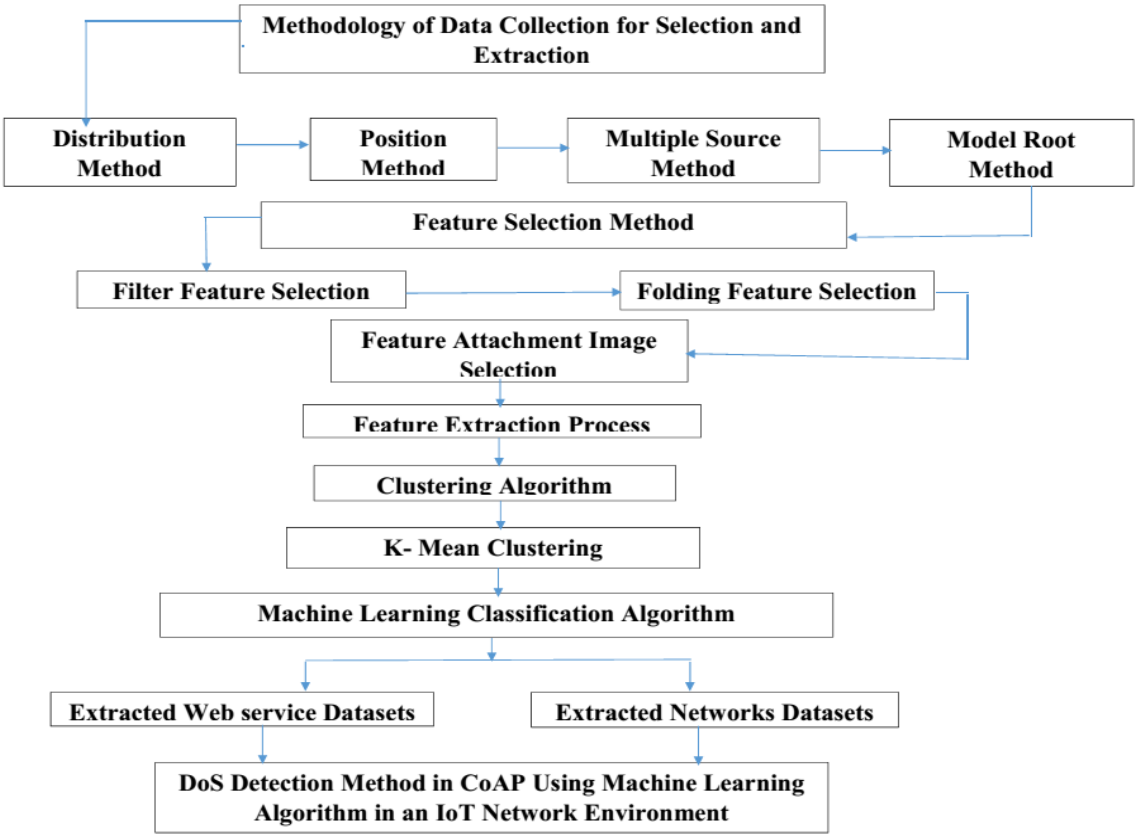

Figure 2. Methodology Designed for DoS Detection in an IoT Network Environment.

The performance of the algorithm is measured by the percentages of rations classified instances obtained from the three algorithms and classifier names. The experiment was run using a feature selection algorithm labeled Feature Selection (FSA), Cluster Algorithm (CA), and K-means Cluster algorithm (K-MCA). A classifier name labeled as Training and Testing, training 0.9 and testing 0.1, 0.7 training and testing 0.3, and, 0.2 training and testing 0.8.

This research addresses the following questions: What is the nature of DoS attacks in the CoAP of the IoT environment? How can a new set of features be identified for detecting DoS attacks in the IoT network environment? How effective is the MLA in detecting DoS attacks in the CoAP of the IoT environment? How does the MLA compare with conventional intrusion detection systems for securing the IoT network environment?

4. Results and Discussion

Observations of the classifier prediction and feature selection algorithm results are very well compared with testing and training ratio scale in Machine Learning for DoS attack Detection in IoT Network Environment using Constrained Application Protocol (CoAP). The classification accuracy process is based on reading the aggregated datasets.

The results obtained from Tables 1 and 2 in datasets classify for training and testing scales as mentioned in the table classification from the three algorithms. Simulation data is presented in Table 3.

Table 1: Classification based on 10-fold cross-validation

Classifier Name	FCA	CA	K-Mean CA
Training (%)	97.66	92.87	98.98
Testing (%)	98.54	95.78	99.56
Classification Accuracy (%)	95.24%	95.23%	99.69%

Table 2: Evaluation of the Generated Classification of Algorithm

Classifier Name	FSA	CA	k-mean-CA
Attack Type	TCP, UDP, and ICMP	TCP, UDP, and ICMP	TCP, UDP, and ICMP
Attack ID	Src IP, Src pt, Dst IP, Dst pt, MAC Address	Src IP, Src pt, Dst IP, Dst pt, MAC Address	Src IP, Src pt, Dst IP, Dst pt, MAC Address
Attack Description	Port Map, LDAP, NetBIOS, Log Attack Ex, Log Attack Int, Clients Conf, Client logs	Port Map, LDAP, NetBIOS, Log Attack Ex, Log Attack Int, Clients Conf, Client logs	Port Map, LDAP, NetBIOS, Log Attack Ex, Log Attack Int, Clients Conf, Client logs
Classification Accuracy (%)	**99.73**	**99.89**	**99.93**

Table 3: Simulation Results

Classification Accuracy (%) of FSA	**The ratio of DoS Request**	**The ratio of DoS Ack**	**The ratio of Wrong URI**	**The ratio of Wrong Accept**
PPMD = 99.73	98.89	0.84	99.71	0.02
PPSD = 99.73	98.86	0.87	98.82	0.91
Classification Accuracy (%) of CA	**The ratio of DoS Request**	**The ratio of DoS Ack**	**The ratio of Wrong URI**	**The ratio of Wrong Accept**
PPMD = 99.89	97.97	1.92	96.98	2.91
PPSD = 99.89	98.83	1.06	99.36	0.53
Classification Accuracy (%) of k-mean-CA	**The ratio of DoS Request**	**The ratio of DoS Ack**	**The ratio of Wrong URI**	**The ratio of Wrong Accept**
PPMD = 99.93	92.87	7.06	95.78	4.15
PPSD = 99.93	95.23	4.7	97.36	2.57

4.2 Performance Measures

The scheme is evaluated using the following metrics. Detection Accuracy is the ratio of the total number of detected malicious messages and the total number of malicious messages transmitted over CoAP. Detection Accuracy of Public-Private Mobile Devices (PPMD) and Public-Private Static Devices (PPSD).

Detection Accuracy = aggregate no. of detected malicious messages + aggregate no. of a malicious message transmitted.

AD = 99.93%

THROUGHPUT

A total number of delivered bits to the server. Maximum TCP Throughput (Mbit/s) 146

DELAY

The total time taken by a message to reach the server node in the network.

Latency or Delay = Propagation Time + Transmission Time + Queuing Time + Processing Delay Latency or Delay =12400000

OVERHEAD

A total number of control messages is used for providing security in CoAP. Max achievable TCP throughput limited by TCP overhead (Mbit/s): 147.1391

4.3 Analysis and Discussion

The results were categorized to simplify the analysis and discussion for a better understanding. Firstly, the Dataset for training and testing and the Evaluation Classification algorithm were obtained based on the accuracy of the three algorithms and simulated in the Cooja Network Platform for the best accuracy and detection ratio. The results from the three algorithms showed a significant performance with overall accuracy for Feature selection at 95.24%, Clustering at 95.23%, and K-means at 99.69%. An evaluation of generated classification algorithm resulted in 99.73%, 99.89%, and 99.93 respectively. K-means algorithm with high accuracy compared with feature selection and clustering.

First simulation for FSA with a percentage of 99.73% for both Public Private Mobile Devices PPMD and Public Private Static Devices PPSD. DoS request was sent from PPMD with a ratio of 98.89% and only 0.84% was acknowledged and 99.71% ratio of Wrong URI was captured and only 0.02% was successfully accepted. In the scenario of PPSD, 98.86% of DoS request was sent only 0.87% was acknowledged and 98.82% was captured as wrong URL only 0.91% for wrong accepted.

The second simulation using CA on the same devices of PPMD

with a ratio percentage of 99.89% send a DoS request to the server, 97.97% was successfully dropped from the request with only 1.92% server Acknowledgement. While 96.98% of Wrong URLs dropped the packets request only 2.91% were successfully acknowledged as wrong accept. The PPSD used the same percentile ratio of 99.89% in the simulation and 98.83% was successfully dropped and detected as a DoS attack, and only 1.92% successfully Acknowledge. The wrong URL also captured packets with a ratio of 99.36% as detected on the wrong URL that is not within the network constrained of CoAP, only 0.53% was successfully server Acknowledge.

The third simulation for k-means CA on (PPMD) in a ratio of 99.93% for DoS attack detection successfully dropped packets 92.87% as DoS request from the client's server only 7.06% was successfully Acknowledged. The same percentage of the 99.93% used on the wrong URL which was dropped identified packet of the wrong URL with a 95.78% only 4.15% was successfully acknowledged by the host configuration server. While the PPSD ratio of 99.93% sent DoS requests and 95.23% was successfully dropped only 4.7% was acknowledged by the server. The wrong URI ratio was 97.36% detected as the wrong URI from the web server only 2.57% was successfully Acknowledgement as wrong accepts of URL which is not within the constrained.

This research contributes to the literature on IoT network security by applying mixed methods of qualitative and quantitative to enhance the security scheme for CoAP in the IoT environment. The focus on DoS attacks and the application of the MLA for detecting them provides a new approach to securing the CoAP in the IoT environment.

5. Conclusion

The research provides an effective approach to enhancing the security scheme for CoAP in the IoT environment by applying mixed methods of qualitative and quantitative to identify and detect DoS attacks. The MLA is shown to be an effective tool for detecting DoS attacks in the IoT network environment, with higher accuracy compared to conventional intrusion detection systems. The findings contribute to the literature on the security of IoT networks and provide a new approach to securing the CoAP in the IoT environment. Performance evaluation and metrics are also discussed. In comparing the performance rates and Accuracy detection for both classification and network simulation environment a k-means algorithm scored the highest percentage in the training and testing of the evaluation and finally in the network simulation platform with the highest percentage of 99.93% in Overall Accuracy.

Reference

[1] Kliarsky, A., & Leune, K. (2017). Detecting attacks against the Internet of Things. SANS Institute Information Security Reading Room.

[2] A10 Network (2021). COAP for Machine-to-Machine Operation [Online]. Available: https://www.a10networks.com

[3] Asim, M. (2017). Security in Application Layer Protocols for IoT: A Focus on COAP.International Journal of Advanced Research in Computer Science, 8(5).

[4] Quakasse, F., & Rakrak, S. (2017). An adaptive solution for congestion control in CoAP-Based group communications. Int. J. Adv. Comput. Sci. Appl, 8, 234-239.

[5] Silverman, M., & Pandey, S. (2018). Wake up radioprotection from denial of service attack Based on baseband monitoring.

[6] Idhammad, M., Afdel, K., & Belouch, M. (2018). The detection system of HTTP DDoS attacks in a cloud environment is based on information theoretic entropy and random forest. Security and Communication Networks, 2018.

[7] Bonguet, A., & Bellaiche, M. (2017). A survey of Denial-of-Service and Distributed Denial of Service Attacks and Defenses in Cloud Computing. Future Internet, 9(3), 43. Retrieved April 15th 2018,fromhttps://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Bonguet%2C+A.%2C+%26+Bellaiche%2C+M.+%282017%29.+A+survey+of+Denial-of-Service+and+Distributed+Denial+of+Service+attacks+and+defenses+in+cloud+computing.+Future+Internet%2C+9%283%29%2C+43.&btnG=

[8] Idhammad, M., Afdel, K., & Belouch, M. (2018). The detection system of HTTP DDoS attacks in a cloud environment is based on information theoretic entropy and random forest. Security and Communication Networks, 2018.

[9] Web Dark. (2017). In Wikipedia, the Free Encyclopedia. Retrieved 17:39, February 28, 2017, from https://en.wikipedia.org/w/index.php?title=Dark_web&oldid=767565229

[10] Jorge, Granjal, João Silva, & Nuno Lourenço (2018). Intrusion Detection and Prevention in CoAP Wireless Sensor Networks Using Anomaly Detection. Sensor, Vol. 18, No. 8 pp. 2445, 2018. Retrieved April 15th 2018, from https://www.mdpi.com/1424-8220/18/8/2445/htm

[11] Daud, M., Rasiah, R., George, M., Asirvatham, D., Rahman, A. F. A., & Ab Halim, A. (2018). Denial of service (DoS) Impact on sensors. In 2018 4th International Conference on Information Management (ICIM) (pp. 270-274). IEEE.

[12] Setikere, S., Sachidananda, V., & Elovici, Y. (2018). Out of Kilter: Holistic

The Exploitation of Denial of Service in the Internet of Things. In International Conference on Security and Privacy in Communication Systems (pp. 43-52). Springer, Cham.

[13] Sicari, S., Rizzardi, A., Miorandi, D., & Coen-Porisini, A. (2018). REATO: REActing to Denial of Service attacks in the Internet of Things. Computer Networks, 137, 37-48.

[14] Sun, H., & Peng, C. (2018). Relaxed Event-Triggered Control of Networked Control Systems under Denial of Service Attacks. In International Conference on AI and Mobile Services (pp. 141-154). Springer, Cham.

[15] Gallais, A., Hedli, T. H., Loscri, V., & Mitton, N. (2019). Denial-of-Sleep Attacks

against IoT Networks.

[16] Al-Hadhrami, Y., & Hussain, F. K. (2019, July). A Machine Learning Architecture Towards Detecting Denial of Service Attack in IoT. In Conference on Complex, Intelligent, and Software Intensive Systems (pp. 417-429). Springer, Cham.

[17] Mamolar, A. S., Salvá-García, P., Chirivella-Perez, E., Pervez, Z., Calero, J. M. A., & Wang,

[18] Biagioni, E. (2019, February). Preventing UDP Flooding Amplification Attacks with weak Authentication. In 2019 International Conference on Computing, Networking and Communications (ICNC) (pp. 78-82). IEEE.

[19] Singh, G., Malhi, S. S., Mahajan, M., Batra, S., & Bath, R. S. (2019, April). Anatomization of Detection and Performance Measures Techniques for Flooding Attacks using Routing Protocols in

MANETs. In 2019 International Conference on Automation, Computational and Technology Management (ICACTM) (pp. 160-167). IEEE.
[20] Rathore, S., Kwon, B. W., & Park, J. H. (2019). BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network. Journal of Network and Computer Applications, 143, 167-177.
[21] Jing, X., Zhao, J., Zheng, Q., Yan, Z., & Pedrycz, W. (2019). A reversible sketch-based method for detecting and mitigating amplification attacks. Journal of Network and Computer Applications.
[22] Anagnostopoulos, M., Kambourakis, G., Gritzalis, S., & Yau, D. K. (2018). Never say never: Authoritative TLD nameserver-powered DNS amplification. In NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium (pp. 1-9). IEEE.
[23] Deccio, C., Argueta, D., & Demke, J. (2019). A Quantitative Study of the Deployment of DNS Rate Limiting. In 2019 International Conference on Computing, Networking and Communications (ICNC) (pp. 442-447). IEEE.
[24] Vyas, A., & Batra, U. (2019). Bot detection by monitoring and grouping domain name server record response queries in DNS traffic. Journal of Information and Optimization Sciences, 40(5), 1143-1153.
[25] Kak, A. (2019). Lecture 16: TCP/IP Vulnerabilities and DoS Attacks: IP Spoofing, SYN Flooding, and the Shrew DoS Attack.
[26] Bhatt, P., & Morais, A. (2018, December). HADS: Hybrid Anomaly Detection System for IoT Environments. In 2018 International Conference on Internet of Things, Embedded Systems and Communications (IINTEC) (pp. 191-196). IEEE.
[27] Adat, V., Dahiya, A., & Gupta, B. B. (2018, January). Economic incentive-based solution against distributed denial of service attacks for IoT customers. In 2018 IEEE International Conference on Consumer Electronics (ICCE) (pp. 1-5). IEEE.
[28] Silva, D., Carvalho, L. I., Soares, J., & Sofia, R. C. (2021). A Performance Analysis of Internet of Things Networking Protocols: Evaluating MQTT, CoAP, OPC UA. Applied Sciences, 11(11), 4879.
[29] Pan, J., Wang, J., Hester, A., Alqerm, I., Liu, Y., & Zhao, Y. (2018). EdgeChain: An edge-IoT framework and prototype based on blockchain and smart contracts. IEEE Internet of Things Journal, 6(3), 4719-4732.
[30] Burke, D. (2018). Preventing DDOS Attacks against IoT Devices (Doctoral dissertation, Utica College).
[31] Wu, C. C., Cheng, R. S., Hsu, C. W., & Wu, L. W. (2019). Lightweight, Low-Rate Denial-of-Service Attack Prevention and Control Program for IoT Devices. Journal of Internet Technology, 20(3), 877-885.
[32] Komninos, Andria, Nikos Procopiou, and Christos Douligeris (2019) ForChaos: Real Time Application DDoS Detection Using Forecasting and Chaos Theory in Smart Home IoT Network. Wireless Communications and Mobile Computing.
[33] Mishra, B. K., Keshri, A. K., Mallick, D. K., & Mishra, B. K. (2019). Mathematical model on distributed denial of service attack through Internet of things in a network. Nonlinear Engineering, 8(1), 486-495.
[34] Hamdan, O., Shanableh, H., Zaki, I., Al-Ali, A. R., & Shanableh, T. (2019). IoT-based interactive dual mode smart home automation. In 2019 IEEE International Conference on Consumer Electronics (ICCE) (pp. 1-2). IEEE.
[35] Ullah, Z., Ahmad, S., Ahmad, M., & Junaid, M. (2019). A Preview on Internet of Things (IOT) and its Applications. In 2019 2nd International Conference on
Computing, Mathematics and Engineering Technologies (iCoMet) (pp. 1-6). IEEE
[36] Silva D, F. S., Silva, E., Neto, E. P., Lemos, M., Venancio Neto, A. J., & Esposito, F. (2020). A taxonomy of DDoS attack mitigation approaches featured by SDN technologies in IoT scenarios. Sensors, 20(11), 3078.
[37] Vipindev, A. & Gupta. B. B. (2018). Security in Internet of Things: issues, challenges, taxonomy, and architecture. Telecommunication Systems, 67(3), 423- 441. Retrieved June 15th 2018, from https://link.springer.com/article/10.1007/s11235-017-0345-9
[38]Kumar, P. M. & Usha, D. G. (2017). Enhanced DTLS with CoAP-Based Authentication Scheme for the Internet of
Things in Healthcare Application. The Journal of Supercomputing, 25(12) 1-21. Retrieved May 5th 2018, from https://link.springer.com/article/10.1007/s11227-017-2169-5
[39] Aljawarneh, S., Aldwairi, M. & Yassein, M. B. (2018). Anomaly-based intrusion detection system through feature
selection analysis and building hybrid efficient model. Journal. Comput. Sci, 25, 152-160. Retrieved April 15th 2018, from https://www.sciencedirect.com/science/article/pii/S1877750316305099
[40] Vander Westhuizen, H. W., & Hancke, G. P. (2018). Practical Comparison between COAP and MQTT-Sensor to Server level. In 2018 Wireless Advanced (WiAd) (pp. 1-6). IEEE.
[41] Haripriya, A. P., & Kulothungan, K. (2019). Secure-MQTT: an efficient fuzzy logic-based approach to detect DoS attack in MQTT protocol for internet of things. EURASIP Journal on Wireless Communications and Networking, 2019(1), 1-15.
[42] Dong, Y., Wan, K., Yue, Y., & Huang, X. (2018). Support Context-Adaptation in
the Constrained Application Protocol (CoAP). In International Conference on Service-Oriented Computing (pp. 294-305). Springer, Cham.
[43] Krawiec, P., Sosnowski, M., Batalla, J. M., Mavromoustakis, C. X., & Mastorakis, G. (2018). DASCo: dynamic adaptive streaming over CoAP. Multimedia Tools and Applications, 77(4), 4641-4660.
[44] Kadam, A., Srivastava, S., Suryawanshi, V., Thorat, N., & Parashar, A. (2018). Network security using constrained application protocol (CoAP). Network security, 3(3).
[45] Jarvinen, I., Pesola, L., Raitahila, I., Cao, Z., & Kojo, M. (2018). Performance
Evaluation of Constrained Application Protocol over TCP. In 2018 IEEE 88th Vehicular Technology Conference (VTC-Fall) (pp. 1-7). IEEE.
[46] Nguyen, J., Yu, W., & Ku, D. (2018). Reliable Transport for Mobile Ad Hoc Networks with Constrained Application Protocol (CoAP) over Negative-Acknowledgment Oriented Reliable Multicast (NORM). In 2018 International Conference on Computing, Networking, and Communications (ICNC) (pp. 361-366). IEEE.
[47] Halabi, D., Hamdan, S., & Almajali, S. (2018). Enhance the security in smart home
applications based on IoT-CoAP protocol. At the 2018 Sixth International Conference on Digital Information, Networking, and Wireless Communications (DINWC) (pp. 81-85). IEEE.
[48] Hameed, S., Khan, F. I., & Hameed, B. (2019). Understanding security requirements and challenges in the Internet of Things (IoT): A review. Journal of Computer Networks and Communications, 2019.
[49] Ioulianou, P. P., Vassilakis, V. G., & Logothetis, M. D. (2019). Battery drain denial-of-service attacks and defenses in the Internet of Things. Journal of Telecommunications and Information Technology.
[50] Gohar, M., Anwar, S., Ali, M., Choi, J. G., Alquhayz, H., & Koh, S. J. (2020). Partial bicasting with buffering for proxy mobile IPV6 mobility management in CoAP-based IoT networks. Electronics, 9(4), 598.
[51] Herrero, R. (2020). MQTT-SN, CoAP, and RTP in wireless IoT real-time Communications. Multimedia Systems, 26(6), 643-654.
[52] Palmese, F., Longo, E., Redondi, A. E., & Cesana, M. (2021,

June). CoAP vs. MQTT-SN: Comparison and Performance Evaluation in Publish-Subscribe Environments. In 2021 IEEE 7th World Forum on Internet of Things (WF-IoT) (pp. 153-158). IEEE.

[53] Bhatt, S., & Ragiri, P. R. (2021). Security trends in Internet of Things: a survey. SN Applied Sciences, 3(1), 1-1