IoT Enabled Line Following Robot

[1]Shrikant Pawar, [2] Shreyas Bhoyar, [3] Samprati Katariya , [4] Om Kalbhor,[5] Swati Jaiswal

Department of Computer Engineering

Pimpri Chinchwad College of Engineering Pune

[1]shri13021998@gmail.com[2]sbhoyar1009@gmail.com[3]samprati.katariya@gmail.com
[4]omkalbhor2804@gmail.com [5]swatijaiswal26@gmail.com

I. Abstract:

The age of the robots is in the twenty-first century. Robots have long been able to bridge the gap between the cybernetic and physical worlds (the internet of things). Because of its impact on all facets of life—including medicine and healthcare, as well as building services, manufacturing, food, production, logistics, and delivery robotics is expected to play a significant role, ever increasingly significant role in society as the most likely contender for the next major industrial revolution's theme, following the current third (digital) industrial revolution.The primary issues here are security, safety, accuracy, and trust. Security mostly has to do with how well-defended these robots are against various cyber-attacks. Trust is based on the degree of satisfaction and ability of these robots to accurately perform and replace humans in certain fields and activities. Safety is related to the reduction of the likelihood of accident occurrence(s).Building on earlier research, growing worries about robots in a multi-robotic environment emerged in the securities industry.When scaled to the requirements, several components, such as sensors, convey enormous amounts of data that are essential for building the data models. The security of sensitive data must be prioritized and taken into account. When transmitting data, it must be encrypted, privacy issues must be considered when utilizing microphones, and transmission signals must be safeguarded.

Keywords: Q learning, Automation, Robot, Arduino, Security, Phototransistors

Paper Received: *20/04/2023* ***Paper Accepted:*** *12/05/2023* ***Paper Published:****05/07/2023*

II. Introduction:

Line path following robot is a system is a one-way machine. The path can be seen as a black or white line in the white or black area respectively. It can be viewed as an ant following a path. It is designed to automatically move and track. The robot uses an LED to indicate a robot. The robot is provided with DC gear Motors to control wheel speed. The vast scope of the problem of finding a way involves efficiency and safety issues. Arduino displays typically use an algorithm to control the speed of the motors directing the robot to move smoothly along the line. In addition, there is an LCD interface that displays the movement of the robot. During the process of designing and studying this robot, we came across a number of potential security flaws that, if not addressed, might result in financial losses when the project is scaled up and used in an environment with several robots. Concerns like these include the safe storage and restoration of data, the upkeep of secure transmission links, and the guaranteeing of confidentiality, integrity, and availability at all times throughout operations.

A. Robotics :

Robotics system is the design of specific devices that can perform physical tasks independently on behalf of humans. Robots often do activities that are either too risky for a human to complete safely. Sensors, actuators, and data processing are used by mechanical robots to interact with the physical environment. A career in robotics requires a good foundation in mechanical engineering, electrical engineering, and computer programming. Most mobile robots feature four wheels or a series of continuous tracks for ease of use. Some scientists have attempted to build more complicated wheeled robots using only one or two wheels. These can provide benefits such as increased efficiency and fewer parts, as well as the ability for a robot to traverse in small spaces that a four-wheeled robot would be unable to do

B. Automation :

“The method of making an equipment, a process, or a system run automatically,” according to the dictionary. However, “the design and deployment of technology to monitor and regulate the production and delivery of products and services” is a more plausible definition. The automation profession includes “everyone involved in the creation and application of technology to monitor and control the production and delivery of products and services,” according to our definition, and the automation professional is “any individual involved in the creation and application of technology to monitor and control the production and delivery of products and services.”

C. Cyber security:

Protecting computer systems, computer networks, and computer programmes from being attacked digitally is the technique known as cybersecurity. These types of cyberattacks often have one of three goals in mind: gaining access to sensitive information, modifying or deleting that information, extorting money from users, or disrupting the regular business process. Any level of your business has the potential to pose a cyber danger. Workplaces must provide cybersecurity awareness training to workers to inform them of typical cyberthreats such as social engineering fraud, phishing, ransomware attacks, and other software used to steal confidential information. Cybersecurity is important across all sectors, not only those with strict regulations like the healthcare sector, as seen by the prevalence of data breaches. Even small organizations run the danger of experiencing irreparable reputational harm after a data breach.

Anomaly Detection in DDoS attack :

The process of discovering unexpected objects or occurrences in data sets, which are distinct from the usual, is referred to as anomaly detection. In addition, anomaly detection, also known as unsupervised anomaly detection, is often used for data that has not been classified. The following are the two fundamental assumptions behind anomaly detection:

- In the data, anomalies only appear on a very infrequent basis.
- Their characteristics are notably distinct from those of the typical examples.

Isolation Forest is an approach for spotting outliers that calculates the anomaly score of each sample by using the Isolation Forest algorithm. This technique is predicated on the idea that anomalies are represented by data points that are uncommon and distinct from the norm. The Isolation Forest model is a hierarchical representation of trees. In these trees, partitions are generated by first picking a feature at random, and then selecting a random split value that falls between the lowest and maximum values of the feature that was first picked.

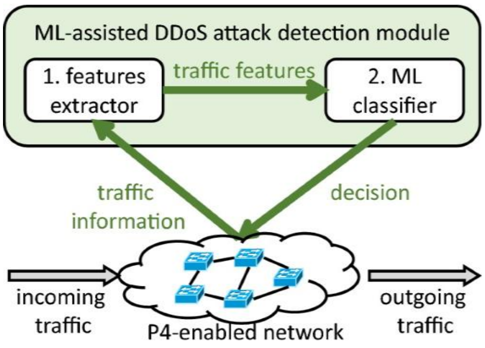


Fig. 1. Anomaly Detection in DDoS attack

III. Background:

A smartphone application with several applications is called Line Following Robot. We looked at many articles outlining the labor involved in creating such a robot. This study has been the subject of a paper. It contains key implementation principles. The most popular gadgets are listed along with a description. The most often utilized sensors for line detection are infrared and ultraviolet. To arrive at precise judgments, a variety of sensors are employed. The most crucial component of the system is the microcontroller, which is in charge of acting after receiving information from sensors in the outside world. PIC and Arduino both function well. The most significant component of this system is the algorithm. Q Learning is the method that offers more efficiency when compared to the others in the papers that we have reviewed. The algorithm used in reinforcement learning is one that relies on feedback.

Some of the difficulties we could encounter include the possibility that robots won't make the proper turn when faced with a T or U angle. Therefore, greater labor is required in these situations. To ensure the proper operation of the robot, security is a crucial issue.

IV.Literature Survey/ Previous Work:

The track that has been drawn on the ground is led by a robot line follower. Mostly black line on a white background. If no obstruction exists or the robot continues to advance along its course. When the robot has a barrier or edge in its path, it will stop. Using. The robot's movement can be simply programmed using computer code and adjusted for various pathways [2].Earlier versions of this type of robot were created for transportation-related industrial automation. With the development of technology, this type of robot is now utilised in Amazon's warehouse management [4].

Sensors, Analog to Digital Converters, Processors, and Motor Drivers are the four fundamental components of electrical construction [16].

Optical sensing : The phototransistors become saturated and begin to conduct when light strikes them. The phototransistor is turned off when no light is shining upon it. The white trail on the black background is illuminated by a white LED. For detecting the white path on the black background, phototransistors are used [9].

Sensor Positioning : An array of sensors is used.The placement of IR sensors must be as exact as possible because they control how the line-following robots move [9].

Robot Steering Mechanism : The algorithm programmed in each microcontroller will determine the steering and movement pattern of the line-following robots. The left and right sensors will pass the current and both motors will be turned ON as the center sensor is shut off when it touches the black line. The middle and right sensors will operate when the left sensor is off to move left, and the right motor will drive the left movement. A right turn will be made using a similar procedure [9].

We have seen the continuous development of autonomous systems over the past few years thanks to the rapid development of artificial intelligence and substantial breakthroughs in Internet of Things technologies. Although exciting, the advancement of autonomous driving technology nevertheless faces fresh difficulties, with security ranking as the main issue.

The sensor itself may pose a threat to this system. The network or range sensors could be disabled by hackers. So intrusion detection system must be used. Zhang et al. (2014) provided a survey for defense tactics and attacks like Sybil attacks in the IoT space. There were three categories of Sybil attacks that the authors identified as SA-1, SA-2, and SA-3 all have a direct harmful impact on IoT's smart objects on performance and privacy data [17]. One paper introduces the Quadratic Line-Detection Algorithm. A quadratic interpolation technique is used to detect the line position more accurately than the other straightforward line-following robots. There were eight reflective optical sensors employed, with the leftmost sensor's coordinate being 0. We had to discover three consecutive sensors with higher output readings than the other five sensors in order to determine where the black line should have been.[18]

V. Mathematical Models :

A. Q-learning for robot kinematics:

After reviewing and comparing the algorithms, the Q-learning algorithm is an algorithm that can be used when accuracy is important. The algorithm is based on reinforcement practice. There are two main types of reinforced learning - Model Based and Model Free, the algorithm mentioned here is Model-Free Learning Algorithm. By completing an in the state and then following the right process, Q * (s, a) is the anticipated value (cumulative discount reward). The temporal variance (TD) is used by Q-Learning to estimate the value of Q *. (s, a). The agent who learns from the environment through episodes without prior knowledge of the environment is the temporal difference. The agent keeps a Q [S, A] table, where S denotes the set of states and A denotes the set of actions..

Q [s, a] represents your current Q * (s, a) estimate state.

Steps in the algorithm:

- Step 1: Initialize the table: The table is a grid of environments depicted in an* n value depicting the environment present around them.
- Step 2: Design actions and enumerate them. For example, for our robot, the actions could be movements right, left, front, etc.
- Step 3: Based on the environment and the movement

are rewarded based on our intuition. For example, since our robot is designed to move in a straight line, the maximum reward is given on forward action.

• Step 4: Update the environment matrix based on the rewards gained. The rewards, in technical terms, are called weights and the environment matrix is called a Q-Table These values can be calculated by simulation using MATLAB to obtain a minimal Q-Table and update values in real-time. Once the values are embedded in the microcontroller, the robot works on a greedy approach and finds a way to find a path with maximum weight.

B. The Quadratic Line-Detection Algorithm

A quadratic interpolation technique is used to detect the line position more accurately than the other straightforward line-following robots. There were eight reflective optical sensors employed, with the leftmost sensor's coordinate being 0. We had to discover three successive sensors that had greater output readings than the other five sensors, as illustrated in Fig. 2, in order to determine the precise location of the black line.

Assume that the three sensors' coordinates are x1, x1+1, and x1+2, and that the true form of the sensors' output values falls within the range [x1, x1+2], which can be approximated by a quadratic curve. Following that, one can discover the following connections between the sensor coordinates and the output values:

$$y_1 = ax_1^2 + bx_1 + c \qquad (1)$$

$$y_2 = a(x_1 + 1)^2 + b(x_1 + 1) + c \qquad (2)$$

$$y_3 = a(x_1 + 2)^2 + b(x_1 + 2) + c \qquad (3)$$

The true position of the line is regarded as the coordinate value at which the output value of the quadratic curve is maximal. One could determine the coordinate value by applying the fundamentals of calculus, which is:

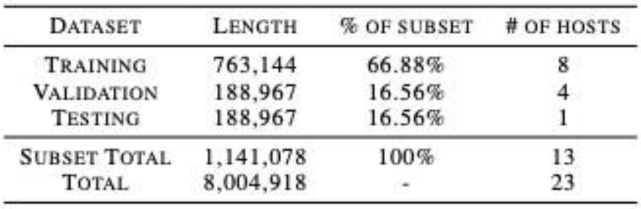
$$x = -\frac{b}{2a} \qquad (4)$$

$$a = \frac{y_1 + y_2 - 2y_3}{2} \qquad (5)$$

$$x = y_2 - y_1 - 2ax_1 - a \qquad (6)$$

It is assumed that the line-following robot's centre position coordinate is 0. As a result, the difference between the robot's centre position and the line position

different sensor logs, which are network traffic and kernel-level process calls. The only items that make up the first benchmark subset are the process logs. Each process call is made up of a total of 14 raw features and 2 labels that have been hand-crafted.



DATASET	LENGTH	% OF SUBSET	# OF HOSTS
TRAINING	763,144	66.88%	8
VALIDATION	188,967	16.56%	4
TESTING	188,967	16.56%	1
SUBSET TOTAL	1,141,078	100%	13
TOTAL	8,004,918	-	23

This would be done under the assumption that an attack is an aberration, or anything that deviates from what is typical, usual, or anticipated.

As a byproduct of the clustering process, it is possible for some clustering algorithms to identify outliers.

Outliers are considered to be items that are located a significant distance from the cluster's centroid, which is the focus of the Clustering techniques. Determining the total number of clusters to use is the primary focus of is attention in cluster-based algorithm design. If there is just one cluster, then the strategy that is based on clusters is going to be quite similar to the one that is

$$e = 0 - x = \quad - x \tag{7}$$

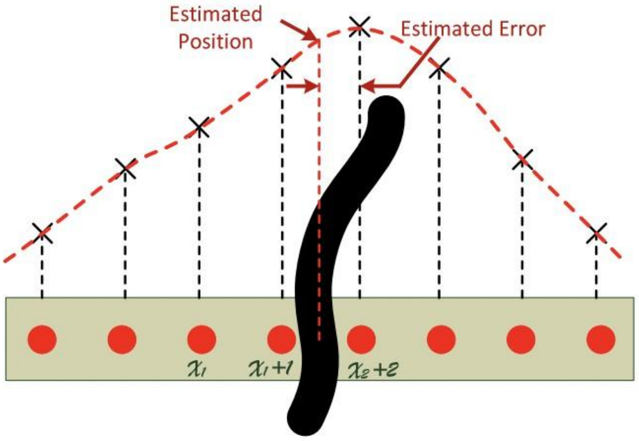


Fig. 2. Line detection via quadratic interpolation.

VI. Proposed Work :

The solution that is being presented has the goal of resolving the problem of DDoS assaults in robotics, particularly in an environment with several robots. Monitoring the internet protocol (IP) addresses and control signals of the robots is crucial to this strategy. It is possible to construct an early method based on the DARPA 99 dataset and to use a clustering technique for anomaly identification.The dataset is made up of two based on distance. If each individual item is considered to be its own distinct cluster, then the cluster-based method will choose outliers in a manner that is completely autonomous.

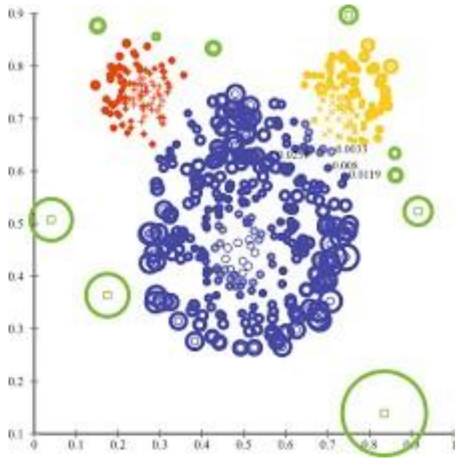


Fig. 3. Clustering

Methods for detecting anomalies that are based on clustering use the assumption that typical data items are members of large and dense clusters, while anomalies are members of tiny or sparse clusters, or they do not belong to any clusters at all. Approaches that are based on clustering may discover such patterns by first extracting the link that exists between the objects and the cluster. A thing is said to be an outlier if it:

- Is the item a member of any particular cluster?

In the event that this is not the case, we refer to it as an outlier.

- Is there a significant gap between the item and the cluster to which it is closest in terms of distance? If you answered yes, then it is an anomaly.
- Is the cluster that the item is a member of a tiny or sparse one? If the answer is yes, then every item that is part of that cluster is an outlier.

There are numerous advantages of such an approach.To begin, they are able to identify outliers without labeling the data, which indicates that they are not in control of the situation. You work with a variety of different kinds of data. You may consider a cluster to be a collection of data in this context. In order for the cluster-based technique to establish whether or not the item in question is an outlier, it is sufficient to simply compare the object in question with the cluster after it has been collected. This procedure is often quite quick due to the very low amount of clusters that are involved in comparison. Regarding the overall quantity of things.

VII. Future Scope :

The current strategy only approaches to overcome problems that arise when a DDoS assault is carried out on a robot, more especially on a path-following robot that is present in an environment with several robots. However, there are a few problems that could occur in the event that the vehicle or robot in question is entirely autonomous. For instance, the sensor data that is kept in a scalable cloud facility has to be protected, and the data itself needs to be encrypted and decrypted according to the specifications of the situation. It is imperative that the robots do not breach any privacy regulations set out by any individuals or businesses. Microphones and speakers, for instance, may listen in on private conversations and record them. In order to effectively manage such circumstances, advanced compression and encryption engines would be necessary to safely store and keep this data without compromising the confidentiality of the information.

VIII. Conclusion:

We can apply these experimental project to a wide range of uses. It can be employed as an autonomous vehicle or an industrial vehicle, and it can be sent to locations where it is difficult or tiresome for humans to access. The performance of the system majorly depends on the algorithm. We analyzed different algorithms which contribute to the efficiency of robots. Security is also an important aspect in the case of automated robots. So security measures need to be taken to avoid attacks like DDoS attacks. The devices used in the robots may get compromised. So in such cases appropriate actions are required to be taken. Different machine learning algorithms are used for anomaly detection.

References:

[1] P. S. Milan, Santosh, S. Das, H. S. Bhanu, “A Review on Self-Balancing Line follower Robot “, *International Journal of Engineering Research & Technology (IJERT)*, January 2021

[2] V. Barua, A. Pathak, Nahar, “An Ultrasonic Line Follower Robot to Detect Obstacles and Edges for Industrial and Rescue Operations”, *International Journal of Computer Applications*, June 2020

[3] Q. T. Sadat, S. K. Rahman, T. E. Nur, N. S. Ferdous, “Design and Implementation of Line Follower Robot using Arduino Microcontroller”, *International Journal of Scientific & Engineering Research*, April 2020

[4] J. Chaudhari, A. Desai, S. Gavarskar ” Line Following Robot Using Arduino for Hospitals”, *International Conference on Intelligent Communication and Computational Techniques (ICCT)*, September 2019

[5] W.H.M. Saad, H.R. Ramli, R. Marimuthu, S.A.A Karim, Z. Manap,” Development of Line Follower Robot with Camera Surveillance System”, *International Journal of Recent Technology and Engineering (IJRTE)*, November 2019

[6] B. N.Mohapatra, K. U. J. Husain, R. K. Mohapatra, ”Implementation of a Line Follower Robot using Microcontroller”, *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, December 2019

[7] M. Srilekha, N. Fathima, G.Anusha, D. S.

Chary "Line Follower Alphabot Using Arduino Micro Controller", International Journal of Engineering Research in Electrical and Electronic Engineering (IJEREEE), February 2018

[8] R. K Sure, S. Patil, "Android Based Autonomous Coloured Line Follower Robot", *International Journal of Research in Engineering and Technology(IJRET)*, eISSN: 2319-1163

[9] S. Shamikh M. Husaini, S. Mohammad Hamza, M. Saalim, “A Comparison based Line Following Robots Design for Path Planning and Maze Solving”, *International Research Journal of Engineering and Technology (IRJET),* Sep 2020

[10] A. Khalique, M. I. Bhatti, “Command Based Line Following Robot using RF Technology”, *Journal of Advanced Computer Science and Technology Research, 2011*

[11] K. Akka, F. Khaber “ Mobile Robot Path Planning using an Improved ant colony Optimization”, *International Journal of Advanced Robotics System (IJARS),* 2018

[12] Y. Wang, W. Zhou, “Reliable Intelligent Path Following Control for a Robotic Airship Against Sensor Faults”, *Institute of Electrical and Electronics Engineering (IEEE),* 2019

[13] D. Liu, HanXvSun, Q. Jia ,“Stabilization and Path Following of a Spherical Robot” ,*Institute of Electrical and Electronics Engineering (IEEE),* 2018

[14] Y. Tao, “A Mobile Service Robot Global Path Planning Method Based on Ant Colony Optimization and Fuzzy Control*“, Institute of Electrical and Electronics (IEEE),* 2021

[15] A. Hassanein, M. Elhawary ,“Robot Path Planning using An Ant Colony Optimization Approach: A Survey”, International Journal of Advanced Research in Artificial Intelligence (IJARAI),2022

[16] M. Pakdaman, M. M. Sanaatiyan,M. R. Ghahroudi, “A Line Follower Robot from design to Implementation: Technical issues and problems
”, *Institute of Electrical and Electronics Engineering(IEEE), 2010*

[17] K. M. A. Alheeti & K. McDonald-Maier, “Intelligent intrusion detection in external communication systems for autonomous vehicles”, *Systems Science & Control Engineering: An Open Access Journal, 2018*
[18]Highnam, Kate, Kai Arulkumaran, Zachary D. Hanif and Nicholas R. Jennings. “BETH Dataset: Real Cybersecurity Data for Anomaly Detection

Research." (2021).

[18] M. Engin1 , D. Engin, "Path Planning Of Line Following Robot",