REPUBLIC OF TÜRKİYE

ALTINBAŞ UNIVERSITY

Institute of Graduate Studies

Electrical and Computer Engineering

A NEW LOCALIZATION MECHANISM IN IOT USING GRASSHOPPER OPTIMIZATION ALGORITHM AND DVHOP ALGORITHM

Shakir Mahmood AL JANABI

Doctor of Philosophy

Supervisor

Asst. Prof. Dr. Sefer KURNAZ

Istanbul, 2023

A NEW LOCALIZATION MECHANISM METHOD IN IOT USING GRASSHOPPER OPTIMIZATION ALGORITHM AND DVHOP ALGORITHM

Shakir AL JANABI

Electrical and Computer Engineering

Doctor of Philosophy

ALTINBAŞ UNIVERSITY

2023

The thesis titled A NEW LOCALIZATION MECHANISM IN IOT USING GRASSHOPPER OPTIMIZATION ALGORITHM AND DVHOP ALGORITHM prepared by SHAKIR MAHMOOD AL JANABI and submitted on 19/04/2023 has been **accepted unanimously** for the degree of Ph.D. in Electrical and Computer Engineering.

____
Asst. Prof. Dr. Sefer KURNAZ

Supervisor

Thesis Defence Committee Members:

Asst. Prof. Dr. Sefer KURNAZ	Department of Computer Engineering, Altınbaş University	________________
Prof. Dr. Osman Nuri UÇAN	Department of Electrical and Electronics Altınbaş University	________________
Asst. Prof. Dr. Abdullahi Abdu IBRAHIM	Department of Computer Engineering, Altınbaş University	________________
Asst. Prof. Dr. Serdar KARGIN	Department of Biomedical Engineering, Arel University	________________
Asst. Prof. Dr. Zeynep ALTAN	Department of Software Enginering, Beykent University	________________

I hereby declare that this dissertation meets all format and submission requirements for a Ph.D. dissertation.

Submission data of the thesis to Institute of Graduate Studies: ____/____/____

I hereby declare that all information/data presented in this graduation project has been obtained in full accordance with academic rules and ethical conduct. I also declare all unoriginal materials and conclusions have been cited in the text and all references mentioned in the Reference List have been cited in the text, and vice versa as required by the abovementioned rules and conduct.

Shakir AL JANABI

Signature

ABSTRACT

A LOCALIZATION MECHANISM METHOD IN IOT USING GRASSHOPPER OPTIMIZATION ALGORITHM AND DVHOP ALGORITHM

Al-JANABI, Shakir

Ph.D., Electrical and Computer Engineering, Altınbaş University,

Supervisor: Asst. Prof. Dr. Sefer KURNAZ

Date: April / 2023

Pages: 57

Nowadays, different types of computer networks such as Wireless sensor networks (WSNs), the Internet of things (IoT), and wireless body area networks (WBANs) transfer information, share resources, and process information. The IoT is a novel network which interconnects various smart devices and can consist of heterogeneous components such as WSNs for monitoring and collecting information. Characterized by specific advantages, the IoT contains different types of nodes, each with few sensors to collect environmental information on agriculture, ecosystem, search and rescue, conflagrations, etc. Despite extensive applications and high flexibility in the modern world, the IoT faces specific challenges, the most important of which include routing, energy consumption and localization. Localization leads to other network challenges and thus can be considered the most important challenge in the IoT. Localization refers to a process aiming at determining the positions and locations of objects lacking global positioning system (GPS) and needing to use the information of network sensors and topology to estimate their own positions and locations. The distance vector hop (DV-Hop) algorithm is a range-free localization technique, in which the major challenge is that the number of hops between two nodes is multiplied by a number that is the same for all nodes leading to a significant reduction in the localization accuracy. In this paper, a network node with no GPS determines the hops from three anchor nodes with GPS. The location of smart objects can be then estimated according to distances from those anchor nodes. Thereafter, a few positions can be created nearby to mitigate the error. Then each position can be regarded as a member of the grasshopper optimization algorithm (GOA) to minimize the localization error. According to the results obtained from implementation of the proposed algorithm, it is characterized by a lower localization error than grasshopper optimization, butterfly optimization, firefly and swarm optimization algorithms. From the results we obtained that the proposed method has high performance than other method and the localization error for the FA, BOA, GOA (Proposed), PSO are DV-Hop are 1.940, 0.530, 0.416, 0.490, and 0.238 respectively.

Keywords: Internet Of Things (IoT), Localization, Grasshopper Optimization Algorithm (GOA), DV-Hop Localization Algorithm, Received Signal Strength Indicator (RSSI), Service-oriented Architecture (SoA).

TABLE OF CONTENTS

Pages

LIST OF TABLES

Pages

LIST OF FIGURES

Pages

ABBREVIATIONS

IOT	:	Internet of Things
WSNs	:	Wireless Sensor Networks
WBANs	:	Wireless Body Area Networks
VANETs	:	Vehicular Ad-Hoc Networks
GPS	:	Global Positioning System
TDOA	:	Time Difference of Arrival
RSSI	:	Received Signal Strength Indicator
AOA	:	Angle of Arrival
GOA	:	Grasshopper Optimization Algorithm

1. INTRODUCTION

1.1 BACKGROUND

Computer networks have been developed and evolved enough, and various types of them are emerging currently. Most of the modern devices are highly intelligent and capable of connecting to the Internet to be considered as Internet members. Smart devices include a group of objects which can have a set of sensors, processors, and even some memory to store basic data and information (Shit et al., 2019). The Internet of things (IoT) is a massive network of various objects, each with a few sensors to communicate with the surrounding environment and to collect different types of information. In this network, each object has important and vital information that can be sent to users, a base station, or a processing system via the Internet. The IoT is also called a heterogeneous network because of having many mismatched objects leading to the higher complexity of the IoT than other types of networks. The IoT can consist of network-like components, and networks such as wireless sensor networks (WSNs) (Saeed et al., 2019)(Alwafi et al., 2021)(Al Hayali et al., 2020), wireless body area networks (WBANs) (H. Wang et al., 2019) and vehicular ad-hoc networks (VANETs) (Balico et al., 2018) can be generally regarded as the components of this massive network. The IoT is used in different areas, and most cities around the world are being developed to become smart. Nowadays, words such as smart cities and smart homes are frequently heard indicating advances of the IoT in these areas. At the same time, the IoT is mainly used in smart transportation and agriculture, and the decreased dimensions of smart objects and sensors have led to easier and more cost-effective implementation of such networks. However, these networks face specific challenges more frequently than other networks because of higher complexity, and it is necessary to develop novel strategies to meet the challenges (Nath et al., 2018). A serious challenge is the large volume of data generated in this network known as big data. In fact, big data are generated due to data collection through sensors or applications in this network. Cloud computing (Huang et al., 2019) and fog computing systems (Mahmud et al., 2018) have recently been employed to process big data. It is impossible to rely on undistributed systems to reduce the computing time of the IoT in which a large volume of data is generated because data are too big to be processed on these systems. Hence, these data are mostly processed in distributed systems such as Apache Spark (Constante Nicolalde et al., 2018). The IoT challenges are not only limited to data size but also related to network routing because of the need for specific methods for optimal data transfer throughout the network.

As well as academic institutions like Ubicomp and PerCam, Mark Weiser's 1991 paper, had an impact on the current conception of the Internet of Things (Friedemann & Floerkemeier, 2010)(Palermo, 2014).

1.2 APPLICATION AREAS

Using these platforms enables municipal residents, local governments, and other stakeholders to collaborate on issues like parking, traffic, and lighting while making better use of their time and other resources. They also facilitate improved waste management.

Applications exist for producing and sharing predicted traffic concentrations for the current or the future. Using smartphone room apps, you can find out which parking spaces are available, how many people are using them, and how much it will cost you to park there. They could offer details on waste disposal techniques like monitoring waste bottle fill rates, enhancing garbage car collecting procedures, shifting container locations, and altering bottle sizes (Aktemur et al., 2020).

Applications for monitoring environmental factors such as air pollution, rainfall, dam roundness, and forest fires are being created in order to take prompt action as necessary. Smart home applications are being developed to give consumers the ability to remotely control and monitor a variety of services provided by their homes, including lighting, heating, ventilation, entertainment, and security, among others.

In order to support procurement procedures, it is being developed to help with the monitoring of products whose typical is running low and whose expiration date is impending, also the replenishing of products, when necessary. It's being created to keep an eye on a number of things, such as temperature and the presence of dangerous compounds in regions where there are animals.

Vast quantities of sensor data (data) are collected from the physical environment, and examination systems are developed that contain the necessary analytical architecture and approaches for communicating the information from the analyzed data to the business layer. IOT tasks include selecting the sensors to use for data collection, selecting the door to use for data transmission to employees, selecting information communication standards, and setting up decision systems (Bhushan & Sahoo, 2020).

The sensors that will be used in the systems could be straightforward devices like RFID tags, straightforward sensors like a camera that focuses on motion is an example of a decision-making and operational system. Another illustration is a thermometer circuit that shows the outside temperature at predetermined intervals.

The period of time that Internet of Things devices retain their data (IoT) system is shown in Figure b 1.1. Preprocessing, storage, and archiving are all optional but necessary procedures that follow the initial production of the data, including aggregation, transmission, and filtering. Although data is created (requested) and consumed (analyzed), the times at which it is created (or requested) and the times at which it is used are during querying and analysis (analyzed). Data collection, aggregation, filtering, and early processing are all communication-intensive online processes. 2013 (Carrez). Offline storage is necessary for a number of tasks, including thorough preparation, long-term storage and archiving, and in-depth processing and analysis. How Internet of Things data is managed and how long it lasts are shown in (Figure 1.1).

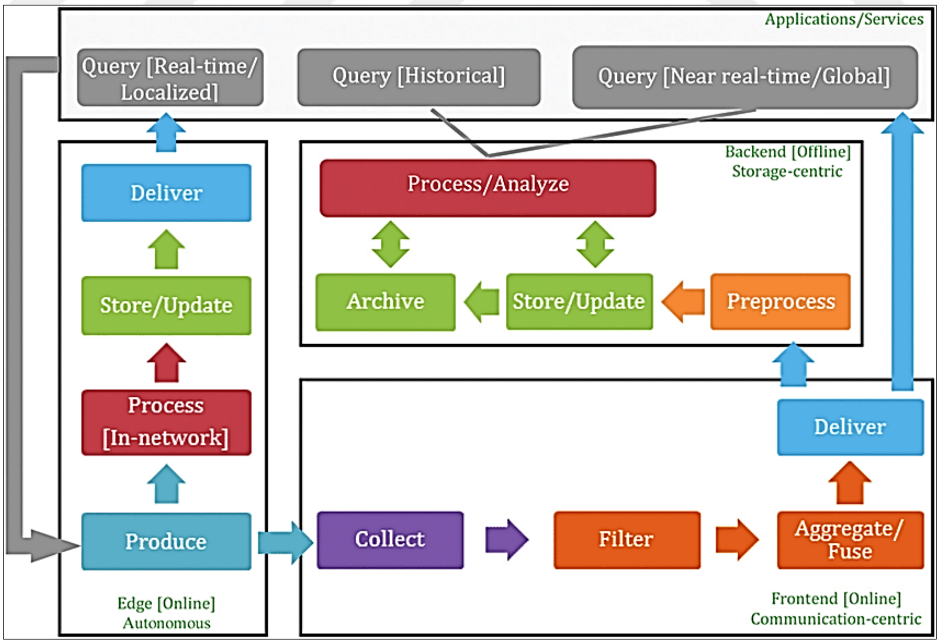

Figure 1.1: Lifetime And Management of Data in The Internet of Things [13].

Whereas archiving is focused on read-only data, storage operations deal with long-term data and updates. The cycle's edges that combine storage and processing components could be separate entities. For localized and real-time services, some IoT devices generate, process, and store data in the network. Below, a detailed explanation of IoT data lifecycle components is provided.

Production: In an IoT framework, data must be sensed, transported, and informed to interested parties on a regular basis (similar to a subscription/notify model). The information is subsequently sent up the network to database servers and aggregation hubs, Alternatively, it is provided in response to inquiries for data obtained by sensors and intelligent objects. Data is frequently geotagged, timestamped, and may have a sophisticated audio/image/video file with a range of levels of sophistication or a simple key-value pair structure.

Data collection: With the Internet of Things, smart devices and sensors may store data indefinitely or report it to controlling elements. At network nodes or gateways, data collecting may take place. After that, it might go through more filtering and processing, possibly being merged into small forms for efficient transport. Zigbee, Wi-Fi, and cellular wireless communication protocols allow items to communicate with collecting points.

Aggregation/Fusion: Due to accelerating data streaming rates and constrained bandwidth, it is getting harder to send the entire network's raw data out in real time. The amount of data that needs to be maintained and transferred is decreased through real-time data summarization and fusion techniques. 2013 (Carrez).

1.3 RESEARCH APPROACH

Localization (Vatansever et al., 2019) is another serious challenge in the IoT because most routing techniques or other IoT protocols operate properly when the positions and locations of nodes are detected correctly. Therefore, it is vital to detect the positions and locations of network nodes in the IoT because the information of objects can be useful when their transfer position is known in the network. In the IoT, the information collected by smart objects depends on their locations, and many of the protocols existing in a WSN can also be used in the IoT provided the fact that every smart object is able to detect its own position. In fact, many of the protocols used for the IoT in a WSN depend completely on the locations and positions of sensor nodes or smart objects. Network routing protocols are among such protocols. It is essential to determine the locations of smart objects in the IoT because the information of each object sent to a base station is valid when the position and location of that object is known. The global positioning system (GPS) (Wu et al., 2019) can be used on each smart object and node in the IoT for localization in specific applications such as urban transportation or search and rescue missions. However, it is very costly to use GPS sensors and equipment for all objects in the IoT, and it is therefore necessary to install these sensors only on some of the objects so that other smart objects use the information of other sensors to determine their locations and positions in the network. A localization method in the IoT is to employ the network information and topology along with the locational information of some network nodes for effective localization of smart objects without using GPS. A few methods have been proposed for localization in the IoT such as the time difference of arrival (TDOA) (Dang et al., 2018), received signal strength indicator (RSSI) (Sadowski & Spachos, 2018) and angle of arrival (AOA) (Vorst et al., 2019).

1.4 RESEARCH MOTIVATION

A major contribution of this study is based on geometric computation that proposed in this paper for smart localization of smart objects in the IoT without imposing the cost of GPS hardware on all network nodes. Metaheuristic algorithms and relevant concepts are then employed to decrease the localization error in DV-Hop and three-anchor methods and to solve an optimization problem. To this end, the IoT and localization challenges are first discussed in this paper. Then the Grasshopper Optimization Algorithm (GOA), used in the proposed method, is analyzed. The proposed method is then modeled using the GOA (Arora & Anand, 2019) to enhance the localization accuracy. Then the proposed method is implemented and analyzed by comparing its localization error with that of other localization methods. Finally, the research results are presented.

1.5 ORGANIZATION OF THE THESIS

There are several portions to this thesis. The first segment covered the problem in detail. The research background's second half focuses on IoT research. The suggested strategy for IoT localization has been developed in the section 4 using the binary version of the grasshopper optimization method, a new method based on grasshopper optimization that had been used in localization.

The fourth and final sections have detailed the implementations and experiments, the suggested strategy and its comparison to other ways, as well as the study findings and potential future directions for creating a recommended algorithm for the localization of the IoT.

2. IOT TECHNOLOGY

2.1 BACKGROUND

In this section, the concepts related to the article for the IoT localization are reviewed. At the beginning of the section, IoT technology is discussing then related studies in the field of localization with approaches such as machine learning and metaheuristic are reviewed. The Internet of things is a new technology for the interconnection of everything. In this technology, everything can be an important network component if it has valuable data to be transferred (Salih et al., 2022)(Darwassh Hanawy Hussein et al., 2022)(Al-Safi et al., 2022). A smart object is a concept used frequently in the IoT, in which every object consists of components for data transfer, data processing, and data storage. Every object can also have a few sensors with the capability of receiving information from the surrounding environment. Furthermore, these objects can also include control sensors to be controlled remotely. In fact, a smart device in the IoT technology refers to an object with different components for information collection and also the ability to send collected information in the network. This object should also have specific hardware components to identify itself in the network (Yaqoob et al., 2019). Depending on their applications, various types of smart objects can be employed in an IoT network. The IoT is a massive network with billions of interconnected computing and sensor nodes exchanging data. The IoT benefits from various technologies such as wireless communications, object recognition based on radio waves, and magnetic tags, etc. (Figure 2.1) shows a schematic view of a massive IoT consisting of different types of smart devices and nodes:

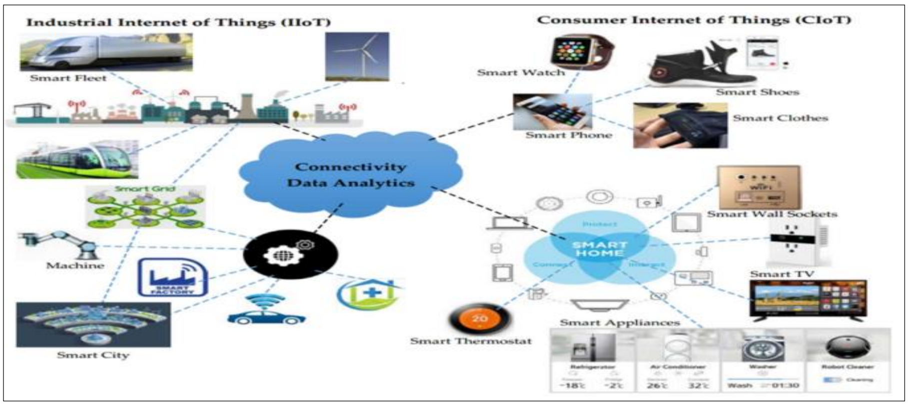

Figure 2.1: A Schematic View of an IoT With Smart Devices and Nodes [34].

As clearly seen, an IoT consists of different types of smart devices and nodes exchanging information with the other components of the network. There are two important parts in the IoT smart object and node (Zheng et al., 2022). A smart object can have a set of nodes exchanging data with its surrounding environment. Any smart object (e.g. a wristwatch) can receive information from sensors and send it to a base station for processing via its communication components. The IoT is a massive network in which various types of sensors are used along with different types of active computer networks; therefore, it is referred to as a heterogeneous network (Motta et al., 2019

Preprocessing: Data from various sources and in various kinds and formats will be produced by the Internet of Things. Preprocessing is necessary for some data before it can be stored. This is done to make sure there are no mistakes, duplicate records, or data gaps. This kind of preparation in data mining is referred to as data cleaning. Schema integration may imply that all data must be placed into a relational (tables) schema, but in reality it refers to a more general idea of a consistent method of accessing data without changing the data types of all sources (s). Applying probability to IoT data items at this step will allow us to adjust for data ambiguity or a lack of trust in data sources (Luo et al., 2009).

Data must be handled, archived, and regularly updated in response to new information according to the duties of this phase. When you get data, you keep it as long as you can without compromising the system's functionality in a non-critical condition. Using storage architectures that may change to accommodate various data kinds and collection rates defines centralized storage. Utilized frequently, relational database management systems arrange data in tables with defined links and metadata for later access (Chen et al., 2010). Since they can store massive volumes (Ramayan and associates 2003).

For autonomous IoT systems, data can be stored decentralized, with the devices that produce it instead of transferring it up the system. Nevertheless, due to these objects' constrained capabilities, their storage capacity is constrained in comparison to the centralized storage strategy.

Processing/Analysis: Around will be an ongoing flow of info that can be utilized to forecast future trends, uncover fresh insights into historical data, or spot data anomalies that call for further investigation. It's critical to remember that this life cycle imposes constraints on conventional data management solutions.

2.2 ADVANTAGE AND DISADVANTAGE OF INTERNET OF THINGS

Every technology in use today hasn't reached its full potential yet. A emptiness exists at all times. So, it follows that the IoT is a significant technology that can aid in the full development of other technologies.

a. The results of automation include task homogeneity, high-quality services, and control over everyday operations without human intervention. Communication between machines aids in maintaining the transparency of processes.
b. Interaction between machines boosts productivity by allowing people to focus on other things.
c. The Internet of Things (IoT) aids in resolving problems related to bottlenecks, malfunctions, and system damage in addition to optimizing energy and resource efficiency.
d. The Internet of Things makes it possible for physical devices to stay connected and communicate more efficiently, leading to better quality control.
e. Having more information available makes it easier to make decisions, which makes life easier to manage.
f. Access to a greater variety of information is made possible by the increasing internet connectivity of our everyday tools, services, and gadgets. It becomes more challenging to protect sensitive information from hackers and other unauthorized users as a result.
g. g. It can be challenging for devices from various manufacturers to connect with one another because there isn't yet a common standard for IoT interoperability.
h. . Due to the size and diversity of the Internet of Things, a single hardware or software error could have catastrophic results.
i. The demand for low-skilled workers in the workplace may decline as the IoT introduces more continual mechanization.
j. By way of our survives become more dependent on technology, society's capacity for basic interpersonal connection will decline.

The Internet of Things has already occupied a substantial place in our daily lives without many of us realizing it. The use of IoT for many of our essential interactions will rise as technology improves and evolves. How much of our daily lives we choose to hand up to technology is totally up to us. But if done correctly, it will adjust to our needs and benefit society as a whole.

You can use intelligent asset inspection to understand how a piece of modern O&C equipment is currently operating. Businesses should employ data from numerous sources, counting SCADA, manual or visual inspections, remote surveillance, subsurface surveillance, aerial surveillance, and remote sensing. The intelligent data for photogrammetry and thermography are then stored using this data, which is built into the desk's back. Businesses can use this to create machine learning algorithms and gather information to aid in decision-making. For instance, companies can utilize intelligent plant inspection to build and manage existing facilities with the use of digital models like digital twins. When model data changes, organizations may use the inspection software as an intelligent resource to maintain a digital twin of an asset. This makes it useful for monitoring in real time and modelling what-if scenarios. In order to keep the model up to date, firms may also conduct inspections using the relevant sensors at the proper frequency. A manufacturing facility or refinery can map its assets and create a digital representation of them using satellites and drones. To generate information and feedback for the purpose of identifying irregularities, Data from both internal and external pipeline data gathering systems and sources may be stored in pop-up memory. IT data for financial and supply chain information may also be used by a smart asset inspection program to improve operational effectiveness across the board for the entire business. The development of numerous solutions for gas and oil applications was then accomplished using a number of IoT and AI-based approaches.

Gasoline tanks may be accessed remotely regardless of their location or movement thanks to IoT technology and its advanced capabilities. Because IoT is a sensor technology, it links to your smart device via communication protocols that also serve as a platform for remotely monitoring tanks. A sensor-based approach forms the basis of the Internet of Things. The cloud platform receives this data after which it processes and stores it before making it accessible to consumers. It consequently permits remote access for users who have specified credentials and personalized settings.

Modern technology called the Internet of Things uses touchscreen gadgets to keep an eye on assets in real time. Businesses can take advantage of this to increase performance and gain a competitive edge. Because of this, IoT technology is used in the construction of the oil and diesel tank monitoring system, enabling a more precise estimation of the fuel level. Put sensors on the tanks so that management may use their networked smart devices to monitor and understand the exact level of the tanks. The system's real-time monitoring capability, which prompts management to receive SMS notifications and modifications, is helpful to a wide spectrum of businesses. As a result, the technology enables managers to take necessary action by enabling real-time monitoring of industrial facilities.

Businesspeople are making strides in several industries, particularly in the petroleum and natural gas sectors. Supply chain management, tank levels, and other areas can now be addressed and covered by the oil and gas industry. Thanks to modern data management and analysis, everything is possible. This makes it possible for companies to monitor preventive maintenance to identify and address asset breakdowns and specific circumstances. The government may utilize this data to forecast planned maintenance and lower operating and maintenance costs. As a result, the company's overall profitability increases, facilitating exponential expansion. Cyber security experts are aware of the problem of intrusion detection, and numerous approaches have been made to solve it. Both the machine learning and deep learning branches of AI can help with the solution to this issue.

2.3 IOT APPLICATIONS

The IoT has different applications and can be used in various fields such as agriculture. Nowadays, smart objects can be placed on farms to control the quality of crops and enhance their productivity by regular monitoring of the status of crops. It is also possible to control the sales network of a product in the market by monitoring the product distribution process. The IoT applications are not limited only to agriculture. According to (Figure 2.2), it can be also employed to enhance and upgrade security, productivity, and smartness to high levels:

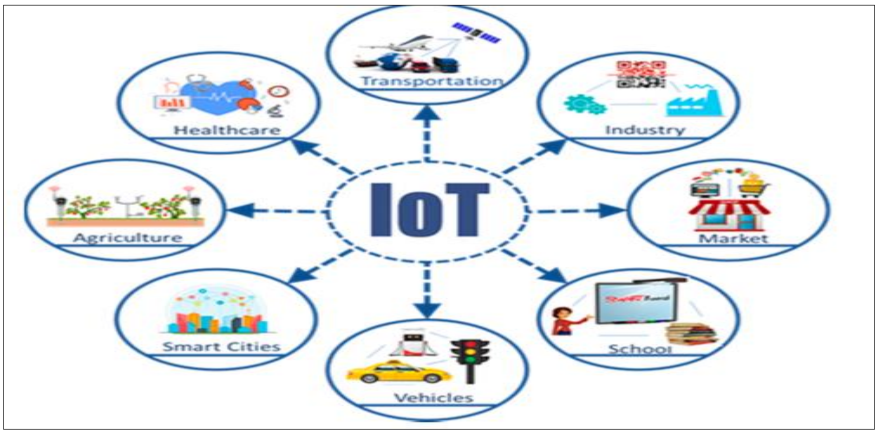

Figure 2.2: The IoT Applications [40].

As seen in (Figure 2.2), the IoT can be used in smart homes and cities, agriculture, transportation, vehicles, healthcare, industries, education and business. A very important application of the IoT is in future smart homes by enhancing comfort greatly. In this technology, a set of nodes are placed in smart homes to collect data from the home environment and to control home appliances.

2.4 IOT LAYERS

As a computer network, different models can be used for communication in the IoT. However, the reference architecture for IoT is a service-oriented architecture (SoA) consisted of a few layers, each provides services to an upper layer. (Figure 2.3), shows three models containing three, four and five layers employed to describe the architecture of IoT :

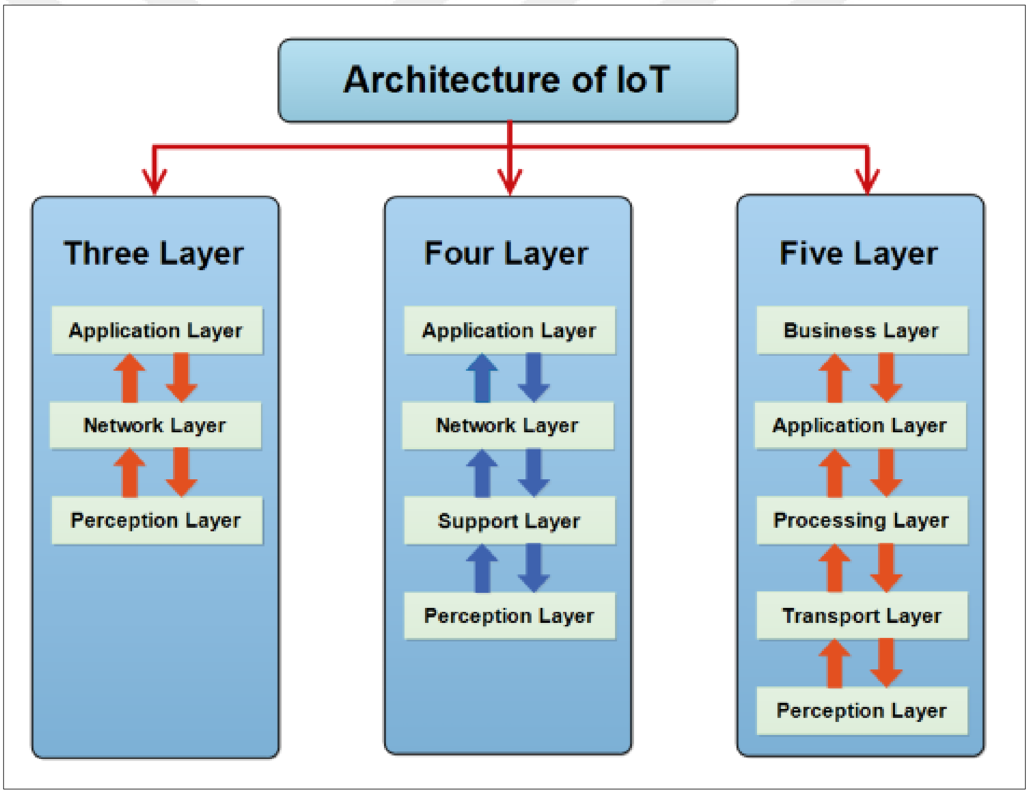

Figure 2.3: Three Reference Models for the IOT.

As seen, the architecture of IoT is defined in business, application, processing and transport and perception layers. There are only application, network and perception layers in some models. However, the perception layer is also called the sensing layer in some cases. Each layer contains a few services which can be provided to upper layers. The perception or sensing layer consists of the sensor hardware protocols such as RFID, RFID readers, intelligent sensors (Zhang et al., 2022), WSNs and Bluetooth. Routing protocols are defined in the network layer, and the software applications of IoT are defined in the application layer.

2.4.1 Identification Technology in IoT

The radio frequency identification (RFID) technology is a method of identifying objects via radio and magnetic waves without a need for direct access to objects for identifying them. In fact, these waves are able to identify objects without direct contact with them. An important application of this technology is in reading the prices of products. This technology can be employed to read and process the data existing in objects. (Figure 2.4) shows an RFID tag for identification of objects in the IoT. Accordingly, these tags have magnetic and local components for information processing. They also have an antenna to send information to a tag reader via radio waves in the IoT:

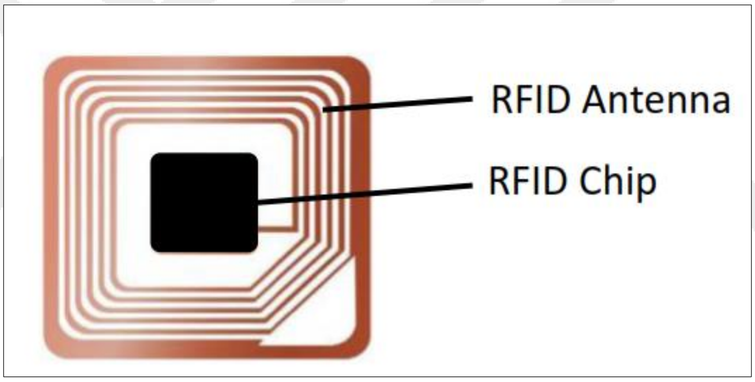

Figure 2.4: An RFID Tag for Object Identification [14]

This technology is actually in competition with barcode readers, fingerprint readers and other similar systems. This technology employs available hardware and software features to obtain the information existing in objects (e.g. prices of products) without direct contact with them. The RFID technology consists of specific components such as an antenna, an ID or a tag, a tag reader, and a software administrator for object identification. Figure 2.5 shows the RFID mechanism for object identification along with the important components used in this technology. As seen, a tag is affected by the radio waves sent by an adjacent tag reader, and then the tag sends identification information of the object placed on it to the tag reader:

Figure 2.5: Activation of an RFID Tag for Identification of Objects in Proximity to a Tag Reader[14].

The RFID technology installs a series of tags on objects for identification, and each tag has valuable information on each object. A tag reader then sends radio waves to tags to activate their information. The tags then send their information to the tag reader. After that, information is sent to a central database on a cloud space or system for analysis. Depending on its applications, a tag reader can have different shapes and structures. There has recently been research on the Internet of Things (IoT). IoT has enormous potential, but it also has a lot of problems. One of the main concerns with the Internet of Things (IoT) is security. This essay examines the growth of IoT research and identifies a number of pressing security concerns. To guarantee data identity and to guarantee heterogeneity, scalability, and Important considerations include accessibility, secure data privacy, confidentiality, integrity, authentication, and access control. These facts are taken into consideration as new IoT solutions are introduced and explored from the technical, academic, and industry perspectives. Designing and deploying IoT solutions that provide anonymity, confidentiality, and integrity in a variety of scenarios is crucial. A complete grasp of why and what security requires cannot be gained by concentrating solely on IoT devices. This crucial IoT security is made up of various parts. IoT security is essential due to the expanding attack surface. Individuals and companies who lack the tools or knowledge to safeguard their IoT ecosystems increase the risks. In addition to the risks themselves, dealing with the consequences of IoT risks is challenging. The IoT is unique in that it has the potential to impact both physical and virtual systems. Internet of Things-related Cyberattacks' outcomes are much more unpredictable due to how easily they can result in physical consequences. Enhancing and safeguarding the network's security Network disruption is a possibility with IoT devices.

2.4.2. Localization in IoT

In the IoT, localization refers to a process in which objects lacking a GPS can estimate their locations and positions through network information and nodes. It is impossible to use the GPS for all objects in the IoT because it is not cost-effective to use this sensor for all objects. In fact, it is impossible to install this sensor on all objects because of a considerable increase in the costs. On the other hand, all objects are not large enough for installation and operationalization of sensors; therefore, only a few objects use the GPS in an operational environment in most cases while the rest of objects lack the GPS and need to detect and estimate their positions and locations with the help of other objects. Figure 2.6 shows a classification of IoT localization proposed by Sadeh *et al.* in 2018. According to this classification, the non-GPS localization methods in the IoT are divided into range-based and range-free localization classes. In the range-based localization methods such as RSSI, TOA, TDOA and AOA, specific information such as distance and angle are used for localization in the IoT. Connectivity, topology, and hops of the IoT are used in the range-free localization methods such as DV-Hop and APIT algorithms.

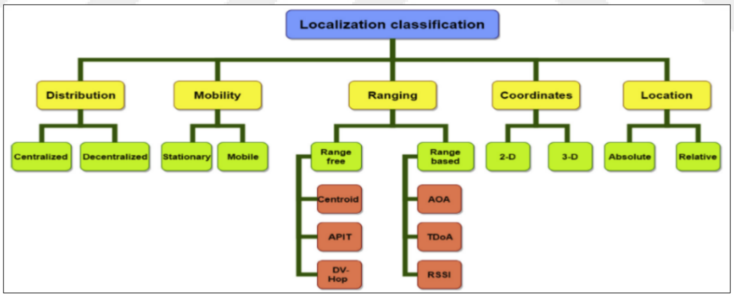

Figure 2.6: Localization Classification in the IoT (Saad Et Al., 2018)

Jeong *et al.* (2018) used an accelerometer and combinatorial information of the IoT, especially the positions of fixed nodes called as anchor nodes, to determine the positions of smart devices and nodes (Jeong et al., 2018). In this method, the information on distances between smart devices and anchor nodes is multicast to a server for estimation. Then the server determines the positions of nodes by using the accelerations of moving devices and the number of hops. A serious challenge in this method is to perform localization on a centralized server, which may reduce scalability of the algorithm.

Wang *et al.* (2018) proposed a hybrid method for localization in the IoT (Lu et al., 2019). They integrated the received signal strength indication (RSSI) with the angle of arrival

(AOA) to determine the positions of nodes and smart devices. In this method, smart devices should have smart antennas to calculate their angles from the existing localizers. The distance is determined through the decreased strength of the sent signal, and triangular ratios are employed to estimate the positions and locations of smart devices.

Khelifi *et al.* (2018) conducted a review study on different IoT localization methods such as AOA, time of arrival/time difference of arrival (ToA/TDoA), RSSI and DV-Hop (Khelifi et al., 2019). They analyzed the distributed and centralized localization in the IoT and also discussed appropriate localization methods in WSNs for use in the IoT. According to their results, it is impossible to propose only a single method for different applications of localization in the IoT. In fact, it is necessary to consider different factors such as accuracy, energy consumption and scalability.

Sotenga *et al.* (2017) proposed a new RSSI-based localization method for estimating the positions and locations of smart devices in the IoT with no access to the GPS (Sotenga et al., 2017). With a further reduction in the signal strength, they were able to estimate that smart object farther from those devices. According to their results, the accuracy of this method was acceptable when many network devices were capable of localization in the IoT.

Hamedani *et al.* (2018) conducted a comprehensive analysis and appraisal of localization algorithms and techniques in WSNs (Hamdani et al., 2018). With their advances in the past decade, WSNs have become very important in wireless networks along with the introduction of the IoT. WSNs consist of sensors aiming at collecting, analyzing and transferring information to a target node/sensor. It is therefore necessary to determine the target levels of sensor nodes. Different programs are employed in WSNs to obtain and use known algorithms and techniques as localization techniques, which help determination of actual positions and geographical locations of sensor nodes. Their study mainly focused on a comparison between different localization techniques in WSNs. This paper can significantly help WSN researchers and practitioners in determining and selecting the proper localization technique according to the WSN requirements.

Gomado and Liu (2019) used metaheuristic algorithms based on the water drops optimization algorithm for localization in WSNs (Gumaida & Luo, 2019). They proposed a high-efficiency metaheuristic algorithm based on a novel optimization method for localization of nodes in an operational environment. This novel optimization method is a nonlinear technique inspired of the behavior of water drops. It was recommended to optimize the target localization performance by using the water drops optimization algorithm to improve RSSI for determining the internal distances of network nodes. Due to specific features in addition to no costs of RSSI, the facile implementation of the proposed method, based on water drops optimization algorithm, has many benefits for the improvement of localization accuracy. According to the simulation results, the proposed algorithm outperformed the ant colony optimization, genetic algorithm and particle swarm optimization in terms of localization.

Kumar *et al.* (2019) proposed and analyzed an RSSI-based method for accurate localization (Kumar, 2019). They evaluated the localization error of the RSSI-based method under hybrid conditions in a complicated environment. Unlike ToA, TDoA and AOA, RSS measurement requires low costs in an interior environment. The experimental results on cellphone localization in two interior environments indicated that they were unusually restricted to the theory. One of the most serious threats to network security that could emerge is infiltration attempts. The ultimate goal of hackers is to fully or partially control the system they are assaulting, and they may employ a variety of strategies to do so. On the other side, information security experts are responsible for protecting the company's digital assets. The defending side also has numerous network and host security tools, including firewalls, IDS/IPS, systems for detecting and preventing data loss, and anti-malware software, to mention a few. Historically, firewalls and Whether used separately or in combination, intrusion detection systems (IDS) acted as the exterior boundary (or border wall) of the protected area (Crichigno et al., 2018). Since network attacks have become more sophisticated and diverse, making it harder to stop them at the enterprise's outer perimeter, recent defensive strategy has changed from stopping intrusions to detecting them. Moreover, due to false positives, direct blocking of suspicious activity may result in a denial of service assault on legitimate traffic (Singh & Singh, 2012). Depending on the data collection technique, host-based IDS checks activity on terminations, specifically hosts. In other words, applications and HIDS monitor system capitals like memory, CPU, to search for odd activity. They have jurisdiction over the host on which they operate to that extent. The bulk of HIDS look for warning signs in places like operating system log files or another piece of software's audit logs (Bhattacharyya & Kalita, 2019). Based on predetermined criteria, alarms are created. They operate rendering to rules, which improves their presentation in identifying known intrusion attempts. Yet, they are useless in spotting fresh assaults. Though sensors are employed in network-based IDS (NIDS) to capture data travelling across networks, they are evaluated to search for anomalous activity (Liao et al., 2013). At the entrance to the secured network, such systems might operate independently while capturing and reviewing every received and departing packet. They might potentially be moved to another part of the network. Traffic from both LAN and WAN can be forwarded to key nodes through the installation of tap devices for analysis. NIDS can function either rule-based or anomaly-based, as will be discussed. Both varieties have benefits and drawbacks. The benefits of HIDS and NIDS are combined in hybrid IDS. This approach promotes the installation of IDS on hosts and nets to look into local events and study system data. At first glance, this idea might seem sensible. On the other hand, managing both systems places a heavier administrative strain on system administrators and information security specialists. On the basis of the methods used to identify assaults, another differentiation is made. IDS that are signature-based or misuse-based identify known threats based on their distinctive behavior (Buczak & Guven, 2015). They defend against acknowledged and well-documented infiltration attempts. Every time a rule is broken for any sort of attack, the IDS needs to be educated to take the appropriate countermeasures. On the other hand, misuse-based IDS has a lot of disadvantages. Simply put, they are unable to recognize unknown or zero-day threats. Even worse, each attack type must be turned into a rule in order to be recognized, suggesting that effective defense requires regular revisions. The most popular open-source, abuse-based intrusion detection systems are Snort, Suricata, and Zeek (formerly known as Bro). When an intrusion attempt is performed to the rule generates an alert if the intrusion attempt occurs more than five times in the space of two seconds. As previously mentioned, if it occurs once every second (or less than five times every two seconds). Already available network scanning and packet creation tools make it simple for intruders to get around such restrictions (Bhattacharyya & Kalita, 2019). Two techniques based on a broad classification of anomaly-based intrusion detection systems are used to make this distinction. First, models are built using statistical techniques by running tests on historical data. Then, the categorization model is compared for each occurrence (Liao et al., 2013). In the following paragraphs, machine learning approaches will be covered in detail. The general public's accessibility distinguishes public data sets from private data sets. Only well-known public data sets will be examined in this study due to the paucity of private sector research. They are commonly used for benchmarking by academics and researchers alike. A lab-generated 1998–1999 data collection is utilized as part of the Defense Advanced Research Projects Agency (DARPA) network security assessment. There is a lot of it since these protocols produce a lot of network traffic. In DARPA's research from 1998 to 1999, the attack types of probing, rootkit, buffer overflow, and denial of service all appear. It features real-world quirks such a lack of false positives and an antiquated network arrangement in the lab, in addition to being outdated and lacking modern attacks (MIT Lincoln Laboratory, 1998). It has attacks like surf and neptune that are different from those of its parents. DoS, user to root, remote to local, and probing are the other four categories of attacks. Nonetheless, it is criticized for having damaged data and being overly repetitive (Cup, 1999). It was proposed to employ NSLKDD to address these issues (Tavallaee et al., 2009). NSL-KDD still has problems because to a dearth of current threats and real-world samples, despite the fact that it reduces statistical flaws in the data set.

Moustafa and Slay presented the UNSW-NB15 data set after realizing the need for a contemporary IDS data set (Moustafa & Slay, 2015). Designing and deploying network attacks in response, these technologies enable the simulation of current attacks. The data collection also contains features obtained from raw data as well as packet capture (pcap) files of flowing traffic. The authors use a bespoke script and the publicly accessible arguments tool to retrieve these attributes. Moreover, a collection of accessible data sets for IDS research has been assembled by the Canadian Institute for Cybersecurity (CIC). They are identified in accordance with the CICIDS format, for instance, CICIDS2017 (Sharafaldin et al., 2018). The CICIDS data sets are produced in a lab environment. The researchers created 25 users using the B-Profile abstraction technique, which resembled human behavior. To guarantee the data set's dependability and completeness, eleven requirements are listed, including a fully equipped accessibility (Serketzis et al., 2019).

Lastly, another company that produces data sets is Stratosphere Lab. We create and compile fictional traffic with malicious, undetectable, and typical profiles. Even though their main focus is attacks, these data sets may contain examples of recent attacks. Few educations using real-world data are available in IDS research, as was previously said, with a few significant exceptions (Bhattacharyya & Kalita, 2019). The majority of earlier research has been done on datasets that were created in lab settings using network traffic simulators and were either public or private. Yet, the following are some disadvantages connected with the usage of intentionally manufactured data sets: (1) The absence specific business network; (2) The absence of real-world dangers in models. The first point could be phrased as follows:

Every organization has a different strategy for designing network infrastructure and providing services. Service X may be provided by Organization A, but not by B or C. Artificially created data sets, on the other hand, make an effort to include all potential attack types because they are created in a controlled environment. In conclusion, real-world traffic training is necessary for corporate IDS models in order to boost their trustworthiness. Since it is generated by simulators, not only is malicious simulated traffic damaging, but even normal traffic does not precisely reflect the behavior of specific business users. Second, attack simulators go out of their way to create attacks that take advantage of well-known weaknesses. But, in a real-world scenario, various payloads might be generated because there will always be additional ways to attack a vulnerability. The most popular implementation, which is also freely available online, is Shteiman's Python script. Unfortunately, there are a lot of different versions of the original script available, even in GitHub's public repositories. With all of these variables, the wildness of the real world may be handled, but manufactured settings cannot.

Table 2.1: Comparison and Analysis of Reviewed Localization Algorithms

Study	Method	Results
(Jeong et al., 2018)	They employed specific features such as an accelerometer, combinatorial information of the IoT, and especially the positions of fixed network nodes called anchor nodes.	Despite acceptable accuracy, this method faces serious challenges including localization on a centralized server, which can reduce the scalability of the algorithm.
Wang *et al.* (2018) (P. Wang et al., 2019)	They integrated the reduced signal strength method with the angle of arrival.	Accuracy is dependent on the use of smart devices with smart antennas to calculate their angles from the existing localizers.
Khelifi *et al.* (2018) (Khelifi et al., 2019)	They conducted a review study on different methods of localization in the IoT.	The main feature of this paper is the analysis of localization methods based on specific indicators such as accuracy, energy consumption and scalability.
Sotenga *et al.* (2017) (Sotenga et al., 2017)	They proposed a novel localization method based on RSSI to determine the positions of network servers.	The accuracy of their method was reasonable when there were many localizable network devices in the IoT.

Table 2.1: Comparison and Analysis of Reviewed Localization Algorithms "Table continued"

Kumar (2019) (Pardini et al., 2019)	In this study, RSS-based localization error identification was performed under hybrid conditions in a complicated environment.	Unlike the ToA, TDoA, and AOA, RSS measurement was of low cost in an interior environment.

2.5 DV-HOP

The distance vector hop (DV-Hop) algorithm is a range-free localization method, in which the distance between two nodes is estimated based on the number of hops. In this algorithm, every anchor node distributes a packet in the network, and other anchor nodes add one unit to the hop field if they receive that packet. Then an anchor node defines the average number of its hops from other anchor nodes in the network as follows (P. Wang et al., 2019):

$$Hopsize_i = \frac{\sum_{j \neq i} \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2}}{\sum_{j \neq} h_{ij}} \tag{2.1}$$

where (x_i, y_i) and (x_j, y_j) are the coordinates of two arbitrary anchor nodes, h_{ij} is the number of hops between the anchor nodes and $Hopsize_i$ shows the average number of hops between the anchor nodes. By calculating the average number of hops in the network, every sensor node determines the number of its hops to an anchor node and then estimates its distance from the anchor node from Eq. 2.2 (P. Wang et al., 2019):

$$d = hop_{pk} * HopSize_i \tag{2.2}$$

(Figure 2.7) shows the mechanism for sending hops and receiving the minimum hops to determine and guess the distance in the DV-Hop algorithm. The following mechanism is used in the IoT to determine the distance between the objects with and without GPS:

a. Objects with GPS calculate the distance from each other, then they determine the number of hops from each other.
b. The average number of hops and distance are calculated in the IoT, and every object without GPS calculates the number hops from those with known locations and positions for localization.
c. It is possible to calculate distances between the objects with and without GPS by multiplying the number of hops by the average distance.

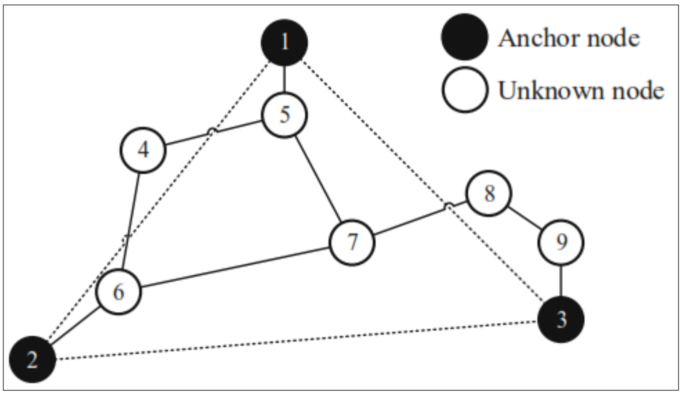

Figure 2.7: DV-Hop Localization in the IoT (P. Wang et al., 2019)

This is a relatively accurate method; however, it increases the network overhead because of sending many packets in different stages of the network. The accuracy of this method is dependent on the density of network nodes and their normal distribution. The accuracy increasing with increasing the density and dispersion normality of the nodes.

2.6 THREE-ANCHOR METHOD

Figure 2.8 schematically depicts three-anchor localization to determine the locations of smart objects through the positions of three anchor nodes:

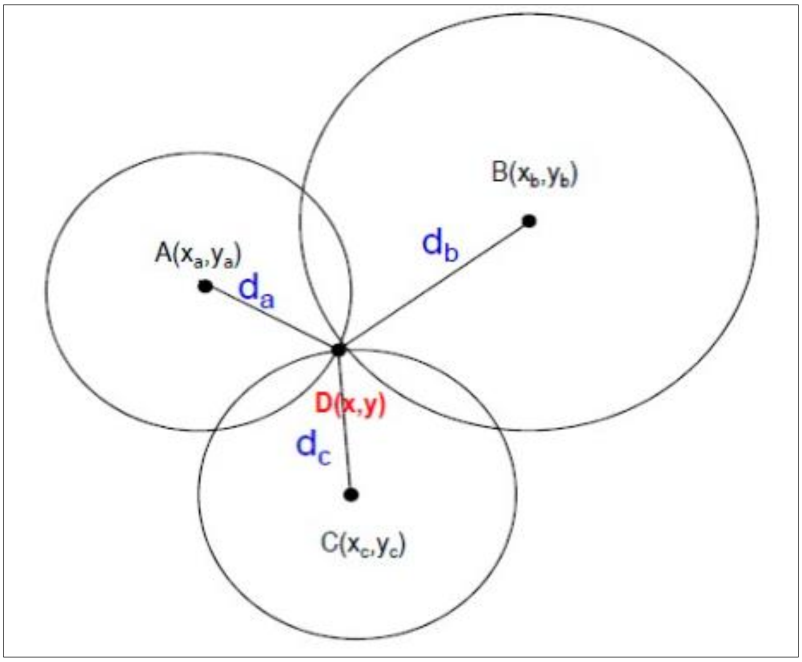

Figure 2.8: Three-Anchor Localization in the IoT (Bae, 2019)

In different computer networks, the large number of hops indicates longer distances, and it is possible to estimate the distance between a node and other nodes in the IoT based on the number of its hops from them. In the three-anchor method, a smart node with no GPS determines its number of hops from those with GPS in the IoT. Based on the number of hops, it then calculates its estimated distance from nodes with GPS and estimates its own position by using the positions of the nodes with GPS through the three-anchor method. As shown in Figure 2.8, it is necessary to have the positions and locations of at least three smart objects in the network. Then an object of interest can estimate its own location by measuring its distances from those three objects and having their positions. The important challenge is that these three points do not necessarily exist within the radio range of the smart device or object of interest. Therefore, it is essential to calculate the distance through methods such as estimation. Assume that a smart object lacking GPS is shown by S_i with unknown coordinates of (x, y), in the proximity of which there are at least three smart objects $A = \{A_1, A_2, A_3\}$ with GPS. Therefore, their locations are known as $\{(x_1, y_1), (x_2, y_2), (x_3, y_3)\}$. The distances of S_i from these objects with GPS, $\{d_1, d_2, d_3\}$, can be respectively formulated through Eqs. 2.3 to 2.6 to measure the distance between S_i at (x, y) and the objects $\{A_1, A_2, A_3\}$ (Bae, 2019):

$$\sqrt{(x - x_1)^2 + (y - y_1)^2} = d_1 \tag{2.3}$$

$$\sqrt{(x - x_2)^2 + (y - y_2)^2} = d_2 \tag{2.4}$$

$$\sqrt{(x - x_3)^2 + (y - y_3)^2} = d_3 \tag{2.5}$$

These three equations can be exponentiated by the power of two and redefined as Eq. 2.6. They can then be expanded to delete the exponentiation factor. To this end, the third equation is subtracted from the first and second equations for simplification, and two equations will be obtained (Eq. 2.7) (Bae, 2019).

$$(x - x_1)^2 + (y - y_1)^2 = d_1^2$$

$$(x - x_2)^2 + (y - y_2)^2 = d_2^2$$

$$(x - x_3)^2 + (y - y_3)^2 = d_3^2 \tag{2.6}$$

$$(x_1 - x)^2 - (x_3 - x)^2 + (y_1 - y)^2 - (y_3 - y)^2 = d_1^2 - d_3^2$$
$$(x_2 - x)^2 - (x_3 - x)^2 + (y_2 - y)^2 - (y_3 - y)^2 = d_2^2 - d_3^2 \tag{2.7}$$

In this equation, the exponential factors y and x can be deleted to obtain an equation and a system of linear equations, which can easily be solved (Eq. 2.8) (Bae, 2019):

$$(x_3 - x_1).x + (y_3 - y_1).y = \frac{(d_1^2 - d_3^2) - (x_1^2 - x_3^2) - (y_1^2 - y_3^2)}{2}$$
$$(x_3 - x_2).x + (y_3 - y_2).y = \frac{(d_2^2 - d_3^2) - (x_2^2 - x_3^2) - (y_2^2 - y_3^2)}{2} \tag{2.8}$$

This equation can be solved to calculate unknown position of a smart object (x, y) and subsequently its location in the IoT.

2.7 GRASSHOPPER OPTIMIZATION ALGORITHM (GOA)

The GOA is a population-based collective algorithm inspired of the migration behavior of grasshopper populations to areas having plenty of food. The behavior of these insects shows a kind of collective and social mechanism among them which leads them to areas of more food. The GOA is based on the behavior of mature grasshoppers because of the highest levels of social interactions in their maturity. Grasshoppers are affected by the following factors when they are flying in nature and migrating toward food resources (Ewees et al., 2018)(Al Shalchi & Rahebi, 2022):

a. Wind
b. Gravity
c. Flying towards areas filled with other grasshoppers

The general equation for the movement of a grasshopper is presented based on wind, gravity and moving toward optimal points (Ewees et al., 2018):

$$X_i = S_i + G_i + A_i \tag{2.9}$$

In this equation, a grasshopper's moving or flying or a solution to optimal points, gravity direction and wind direction are shown by the variables S_i, G_i, and A_i. It can be said that the position vector of a grasshopper or its corresponding solution is updated on the basis of the above three factors. It is assumed in the GOA that every solution is a coded grasshopper which can search the problem domain to find the optimal position of food using the position of the target. In this equation, a change in the positions of grasshoppers is shown by the optimal social position vector,

gravity vector and wind vector (S_i, G_i, and A_i). Equations (2.10), (2.11) and (2.12) can be used through mathematical modeling to model the vectors S_i, G_i and A_i (Saremi et al., 2017):

$$S_i = \sum_{j=1}^{N} s(d_{ij}) \, . \, \widehat{d_{ij}} \tag{2.10}$$

$$G_i = -g\widehat{e_g} \tag{2.11}$$

$$A_i = +u\widehat{e_w} \tag{2.12}$$

where d_{ij} shows the distance between two arbitrary grasshoppers, $\widehat{d_{ij}}$ the unit vector used for the movement of a grasshopper and $s(d_{ij})$ is the jump control function of a grasshopper. The vector distance between two grasshoppers, their unit vector, and their jump functions and steps can be defined with the equations (2.13), (2.14) and (2.15) (Saremi et al., 2017):

$$d_{ij} = \left|X_i - X_j\right| \tag{2.13}$$

$$\widehat{d_{ij}} = \frac{X_i - X_j}{d_{ij}} \tag{2.14}$$

$$s\left(d_{ij}\right) = f e^{\frac{-r}{l}} - e^{-r} \tag{2.15}$$

where X_i and X_j are the grasshopper's vector at the i^{th} and j^{th} positions, respectively, and $s(d_{ij})$ is a jump controller function in the GOA. Moreover, *f* and *l* are the coefficients of attraction of a grasshopper to an optimum and the scale or size of a grasshopper's jump or its equivalent solution when *r* is the distance between the two grasshoppers *i* and *j*. According to Figure 2.9, every grasshopper can consider and show two major reactions to move in the problem domain: attraction force and repulsion force. In fact, a grasshopper searches the space nearby the target in the problem domain

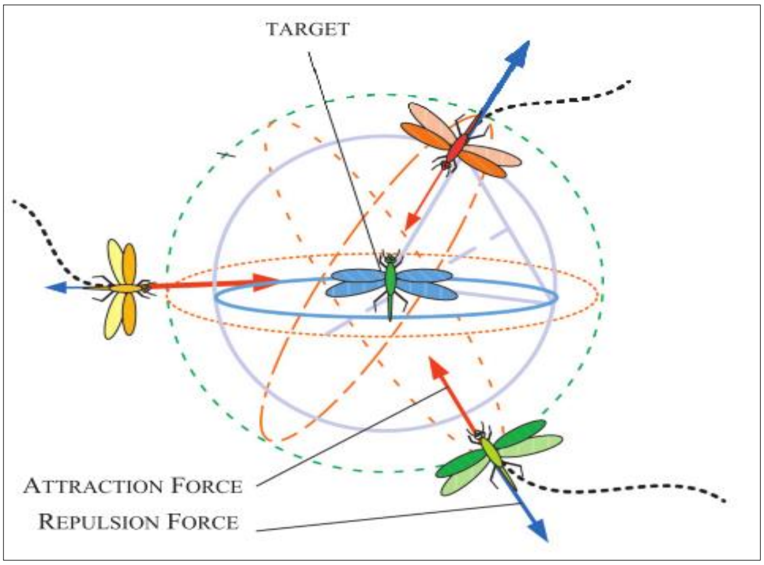

Figure 2.9: The Search Mechanism of Grasshoppers in The Proximity of a Target (Mirjalili Et Al., 2018)

As seen, there are two types of grasshoppers, the first type is attracted to the target. This force is shown by a red vector. The second type includes the grasshoppers which search the surrounding area of the target. Highlighted by a blue arrow, these grasshoppers do not necessarily search the area around the target. In fact, some grasshoppers perform a local search around the optimal grasshopper, i.e. the target, and some other grasshoppers perform a global search farther than the target. According to the evaluation results, the GOA calculates the target with a lower error than other algorithms such as the genetic algorithm, particle swarm optimization, bat algorithm, firefly algorithm and gravitational search.

3. PROPOPSED METHOD

Localization is important because data and information are valuable when it is possible to detect their positions. For instance, the information of objects is important in cases such as conflagrations or search and research when the positions and locations of objects and sensors are identified properly. Localization plays a key role in routing algorithms in IoT, and it is necessary to propose specific methods for developing a low-cost localization algorithm with a lower error. Efforts were made in this study to employ the tags used in objects to identify their positions and locations. For this purpose, these object tags search for three anchor objects with GPS nearby. Then they calculate their distances from them. Based on the positions of those three objects with GPS, the tags determine their locations and positions. However, this method faces a challenge, and there may be less than three objects with GPS in the radio wave of a tag. The hop information was used in this study to deal with this challenge. In the proposed method, if there are fewer than three smart objects with GPS around an object of interest, then it can calculate its distances from those smart objects by measuring the hops using the distance regression based on the number of hops obtained from the DV-Hop algorithm. Then that object can determine its position and location. In the proposed method, localization is carried out based on the DV-Hop algorithm which is sensitive to the network density and may lead to a decrease in the localization accuracy. Moreover, localization may be associated with errors if it is performed through distance regression and hops in the same way as the DV-Hop algorithm. As a result, the localization accuracy may decline. Therefore, it is recommended to employ metaheuristic algorithms to mitigate the localization error, regarded as an optimization problem. Considering the high accuracy of swarm intelligence systems among metaheuristic methods, localization error was mitigated using metaheuristic techniques in the proposed method. Regarding localization in the IoT, the important challenge lies in the fact that it is impossible to install GPS sensors on all objects because of an increase in the implementation cost of the IoT. Furthermore, the GPS does not operate properly indoors in areas such as shops and warehouses leading to an increase in the localization error.

A low-cost localization method is to use the minor features of objects to find their positions and locations. For instance, it is possible to place inexpensive tags such as RFID tags on all objects. Information of objects including prices of products can be inserted on these tags, which can be used for unmovable objects by mentioning the position of each object on it.

However, every smart object can move within a specific range such as in a shop or warehouse in most applications of the IoT. These tags can be employed for the localization of smart objects provided that they interact with other smart objects in the IoT. It is assumed in the proposed method that each object has an RFID tag which could be activated in contact with localization waves and follow these steps for localization:

a. An object without GPS is stimulated by radio waves to estimate its location and position with the help of IoT infrastructures if necessary.
b. The RFID tag of the object is activated to send signals to adjacent objects with GPS.
c. If the nearby smart objects have GPS, they respond to radio waves and send a feedback signal to the object.
d. If an object knows nothing about its position and location, it calculates its distances from three smart objects with GPS by sending and receiving signals.
e. The object of interest uses the three-anchor method to estimate its location and position and calculates its distances from at least three objects with GPS.

3.1. THE PROPOSED STEPS

The proposed method introduces a novel localization mechanism for objects existing in the IoT. In this localization mechanism, geometric and mathematical equations are used along with distance estimation based on hops. The GOA is then employed to improve the localization accuracy. Figure 3.1 shows the proposed steps for localization. Accordingly, if there are at least three smart objects around one smart object with GPS, it faces no challenge in finding its own position. To this end, it can calculate its distances from these three nodes using the sending and receiving times of signals. Having the positions of at least three smart objects and distances from them, it can then estimate its own position. In the second case where there are less than three smart objects with GPS around a smart object without GPS, the object cannot perform localization in the same way as previous steps. It is therefore necessary to estimate its distance from smart objects with GPS and count the number of hops from them. Like the DV-Hop algorithm, it can measure and estimate the distance based on the number of hops.

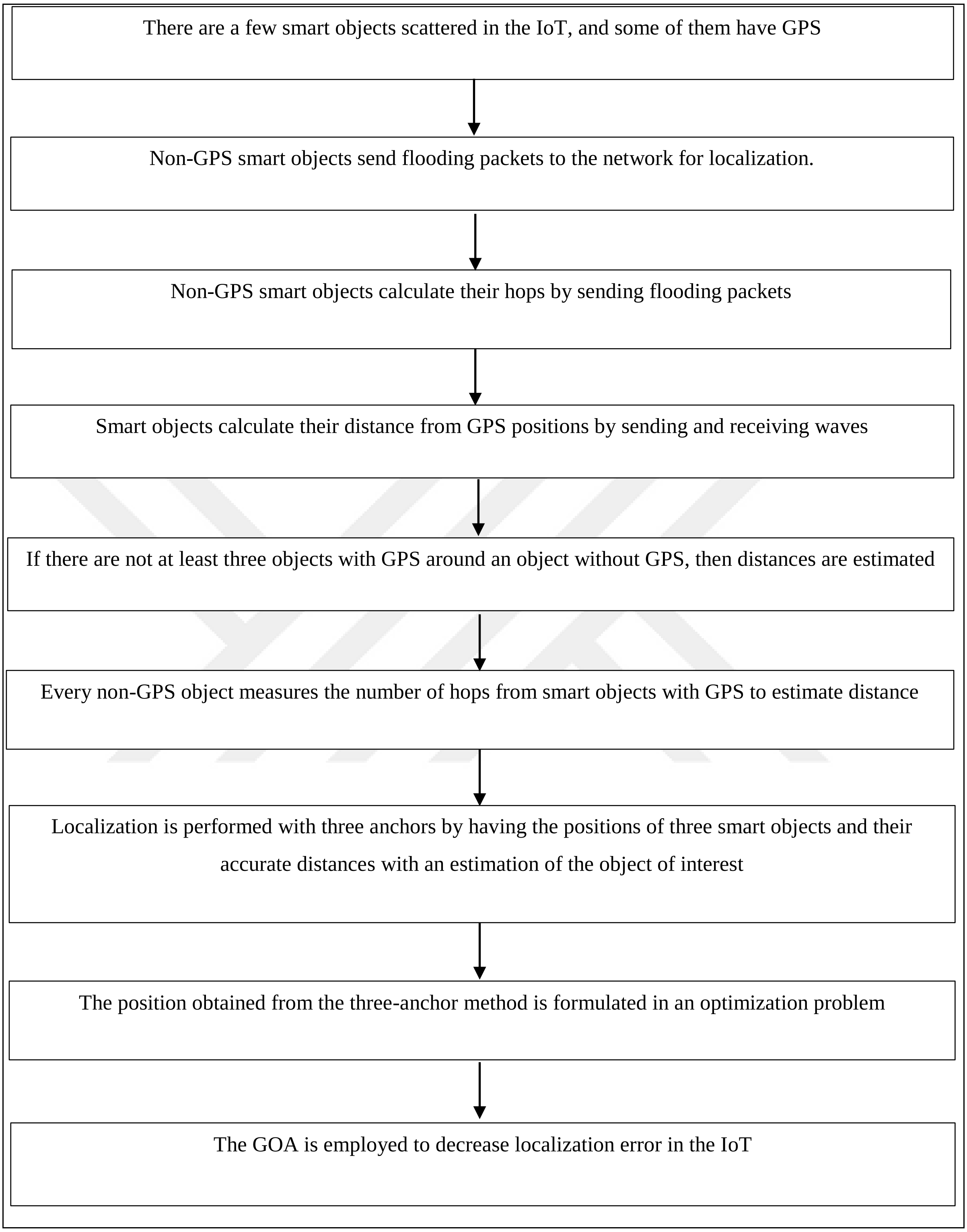

Figure 3.1: Steps of the Proposed Method for Localization in the IoT

Accordingly, the following steps are used for localization in the IoT:

a. First a smart object with no location and position is activated by tag readers for localization. Then this object starts the localization process.
b. The smart object searches its surrounding area and calculates its distance from smart objects in specific positions. In this case, one or two objects exist nearby.
c. The smart object measures its distance from other smart objects with GPS existing outside its radio range by sending hops and estimating distance in the same way as the DV-Hop algorithm.
d. The object of interest sends a few flooding packets in the network to estimate its distances from them by measuring the number of hops and smart objects with GPS.
e. The position and location of the object can be estimated by measuring its distances from three smart objects with GPS and also having their positions through the geometric three-anchor method.

The estimated position of the smart object can be prone to significant errors, which can be reduced by using metaheuristic methods. In this study, the GOA was employed because of its higher accuracy than other well-known algorithms such as the genetic, particle swarm optimization, bat, firefly and gravitational search algorithms. The GOA creates new positions around those obtained by the three-anchor method. In fact, the GOA tries to create new opportunities nearby to perform the localization of the smart object at a lower error.

3.2 MEASURING DISTANCE BETWEEN A NON-GPS OBJECT AND GPS OBJECTS IN THE PROPOSED METHOD

In the proposed method, a non-GPS object requires information on the positions of three objects with GPS and its distances from them for localization. However, it is not always possible to find the three distances because GPS objects may not exist within the range. It is therefore possible to use the hop and distance regression. For this purpose, the number of hops is used for estimating the distance between a non-GPS object and a GPS object outside the range for subsequent use in the three-anchor model. The following steps should be taken to measure the distance between a non-GPS object and a GPS object existing outside the radio range in the same way as the DV-Hop algorithm:

a. The RFID tag of a non-GPS object is activated to detect nearby GPS objects. If possible, the distance is estimated by sending and receiving signals to and from three GPS objects.

If three GPS objects are not found, then the hop and distance regression method is employed.

b. A GPS object sends multicast packets in the network to calculate the number of its hops from other nodes and objects.
c. A GPS object calculates its distance from other GPS objects. It is possible to determine the number of hops on distance based on the number of hops and average distance.
d. Smart objects with no GPS calculate the number of hops from objects with GPS.
e. It is possible to estimate the distance between non-GPS and GPS objects by calculating the number of hops between them.
f. The three-anchor method can be employed to estimate the position of a non-GPS object by estimating the distance between that object and GPS objects.

3.3 THREE-ANCHOR LOCALIZATION IN THE PROPOSED METHOD

In the proposed method, a smart object first tries to find three anchor nodes within it's radio range. If they are found, a signal is sent to each of them. Then it receives the delayed feedback of each signal. Based on the delay, it can then calculate its distances from these three nodes. Since the positions of anchor nodes are available, the smart object is able to calculate and estimate its position and location. Assume that the position of a smart object in the IoT is $(x\ , y)$, regarded as the unknown coordinates in the localization problem. The smart object of interest is characterized by the positions of three anchor nodes: $(x_1\ , y_1)$, $(x_2\ , y_2)$ and $(x_3\ , y_3)$. It can then estimate its distances from these nodes: d_1, d_2, and d_3. The sensor node at $(x\ , y)$ can calculate its Euclidean distances from three anchor nodes in a WSN to solve the system of linear equations by solving the three-anchor equation. Equation 3.1 can be employed to obtain the coordinates of the smart object $(x\ , y)$ in the IoT:

$$\begin{bmatrix} x \\ y \end{bmatrix} = \frac{1}{2} . \begin{bmatrix} (d_1^2 - d_3^2) - (x_1^2 - x_3^2) - (y_1^2 - y_3^2) \\ (d_2^2 - d_3^2) - (x_2^2 - x_3^2) - (y_2^2 - y_3^2) \end{bmatrix} . \begin{bmatrix} x_3 - x_1 & y_3 - y_1 \\ x_3 - x_2 & y_3 - y_2 \end{bmatrix}^{-1} \tag{3.1}$$

In this equation, the unknown position of a smart object is calculated using the positions of anchor nodes and their distances in the IoT

3.4 REDUCTION OF THREE-ANCHOR LOCALIZATION ERROR USING THE GOA

The distance and hop measurement algorithm can be employed in the three-anchor method to partly estimate the position and location of a smart object in the IoT. However, this method is prone to significant errors because the DV-Hop model is not very accurate. In fact, its accuracy depends on the density of nodes in the network. If the currently estimated position of a smart object is $(x\ ,y)$ in the IoT and the three-anchor method, a few coordinates can be obtained from Eq. 3.2 within a specific radius (R) around the smart object:

$$\begin{bmatrix} x' \\ \\ y' \end{bmatrix} = \begin{bmatrix} x + (x \pm R) \times rand(0,1) \\ \\ y + (y \pm R) \times rand(0,1) \end{bmatrix} \tag{3.2}$$

This set of new coordinates, created nearby $(x\ ,y)$, can be regarded as the set $\{(x_1, y_1), (x_2, y_2), \dots, (x_N, y_N)\}$ and used as a member of the population in the GOA. Each of these solutions can be evaluated through Eq. 3.3:

$$J = \left\| \sqrt{\Delta x^2 +\ \Delta y^2} - v.\Delta t \right\| \tag{3.3}$$

where $\sqrt{\Delta x^2 +\ \Delta y^2}$ is the distance between a member of the GOA and an GPS anchor node, and $v.\Delta t$ shows the distance between a solution or position of the anchor node based on the time taken by a signal to leave the smart object, meet the anchor node, and return. In the proposed method, a population of solutions is taken into account to apply the GOA. This solution is used as the population of the GOA to find an optimal solution to reduce the localization error. A few coordinates are first generated in the 2D space to create a population of grasshoppers, each of which is put into the localization objective function for evaluation to find optimal positions. Figure 3.2 shows a framework for this case:

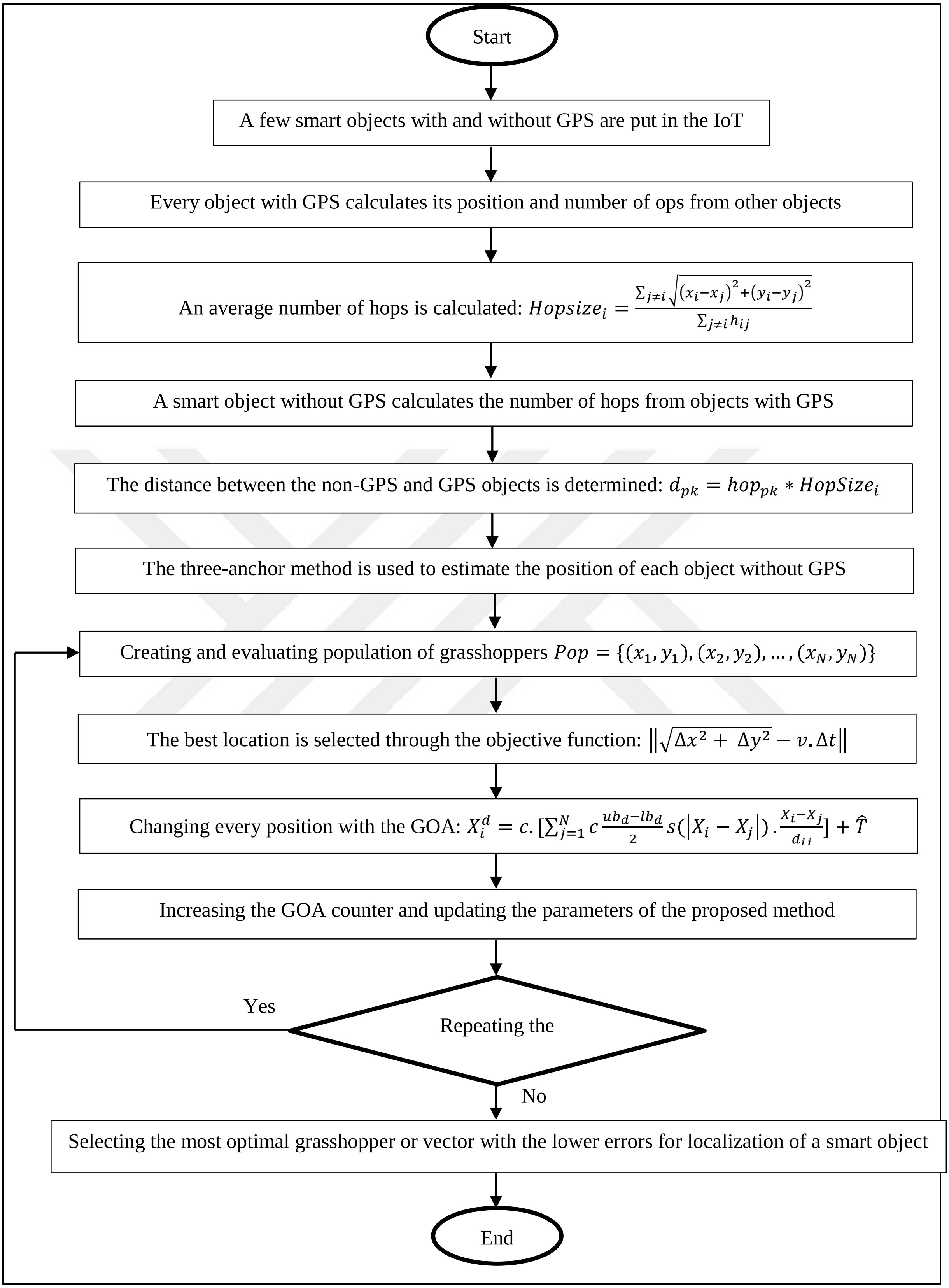

Figure 3.2: The Proposed Flowchart for Localization Improvement with the GOA

In the proposed method, the GOA can be employed to improve the localization of a smart object without GPS and modify its position. To this end, some smart objects with and without GPS are first distributed in the IoT. Every smart object with GPS calculates its number of hops from objects with GPS by multicasting and announces its position to all objects. In the next step, an average number of hops is created through the DV-Hop algorithm. In fact, a non-GPS object calculates its number of hops from at least three GPS objects by multicasting packets in the network. Then every object with GPS multiplies its number of hops from objects with GPS by the average number of hops and distance to estimate its distance from them. Every object without GPS uses its distances from three smart objects with GPS and their positions to estimate its own position. This process is prone to errors. Then a few positions are generated nearby the estimated position for use as the population in the GOA through Eq. 3.4:

$$Pop = \{(x_1, y_1), (x_2, y_2), \dots, (x_N, y_N)\} \tag{3.4}$$

where (x_i, y_i) is a population member of the GOA evaluated by the evaluation function *J* to determine its fitness value. Every coordinate with the lowest error is the most optimal grasshopper in that iteration. It is assumed in the proposed method that the most optimal coordinates are (x^*, y^*) in the current iteration. This position is employed to update and decrease the localization errors through Eq. 3.5:

$$x_i, y_i) = c.\left[\sum_{j=1}^{N} c\frac{ub_d - lb_d}{2} s\left(\left|(x_i, y_i) - (x_j, y_j)\right|\right).\frac{(x_i,y_i)-(x_j,y_j)}{d_{ij}}\right] + (x^*, y^*). \tag{3.5}$$

In this equation, (x^*, y^*) is the position of the most optimal grasshopper or the coordinates of population. Moreover, ub_d and lb_d show the upper and lower limits of dimension *d* of the objective function and *c* indicates the convergence coefficient in the GOA. As defined in Eq. 3.6, it is a descending function of iteration:

$$c = cmax - l\frac{cmax - cmin}{L} \tag{3.6}$$

where *l* and *L* respectively show the current iteration and maximum iteration of the GOA, and *cmax* and *cmin* are equal to 1 and 0.0001, respectively. The GOA is repeatedly executed to decrease localization error, and the average localization error frequently decreases.

4. EXPERIMENTAL RESULTS AND DISCUSSION

4.1 RESULTS

In this section, the important and effective parameters of the proposed algorithm and its implementation are introduced to evaluate its accuracy and efficiency. Then an implementation and operational environment is introduced for the localization of smart objects. Localization evaluation indicators are then discussed. Then a few tests and outputs are discussed, analyzed, and evaluated.

4.2 IMPLEMENTATION AND ANALYSIS PARAMETERS

There are a few important parameters in the implementation of the proposed method. They need to be initialized properly to minimize the localization error. Table 4.1 shows the important implementation parameters of the proposed algorithm for localization of smart objects in the IoT. Some of these parameters are considered to be variable to determine their roles in decreasing and increasing localization errors in the proposed method:

Table 4.1: Implementation Parameters of the Proposed Algorithm for Localization

Parameter	Description and Proposed Value
n	The initial population size of the GOA, which was assumed to be 5, 10, 15.
MaxIt	The maximum iterations of the proposed algorithm (=100).
Run	The number of tests required to obtain results in each case (=50).
VarMin	The minimum radius for a new position around the current position (=0.1).
VarMax	The maximum radius for a new position around the current position (=3)
Cmax	The final parameter of maximum convergence in the GOA (=1).
Cmin	The initial parameter of maximum convergence in the GOA (=0.0004).
Network	The network dimensions (=100*100)
N	The number of objects without GPS in the IoT, which was assumed to be variable.
M	The number of objects with GPS in the IoT, which was assumed to be variable.
R	The radio radius of every smart object (=10 m).

4.3 IMPLEMENTATION AND SIMULATION ENVIRONMENT

In implementations, every object with GPS and without GPS is respectively shown by ☐ and ○. The estimated position is displayed by *. In this study we used the data that was setup randomly in the area, all information and the location of the sensors setup randomly depending on the position of the area. For the implementation and simulation of the proposed method, a 100-m^2 environment was first selected. Then a few objects with and without GPS were randomly distributed in the simulation environment. The objects with GPS can directly determine their positions, whereas those without GPS can perform localization with the help of objects with GPS. The estimated locations of objects are shown by *. Figure 4.1 shows an instance of the implementation and simulation environment for the proposed method with smart objects with and without GPS. In addition, Figure 4.2 indicates the reduction in the localization errors of all smart objects based on the iteration of the GOA:

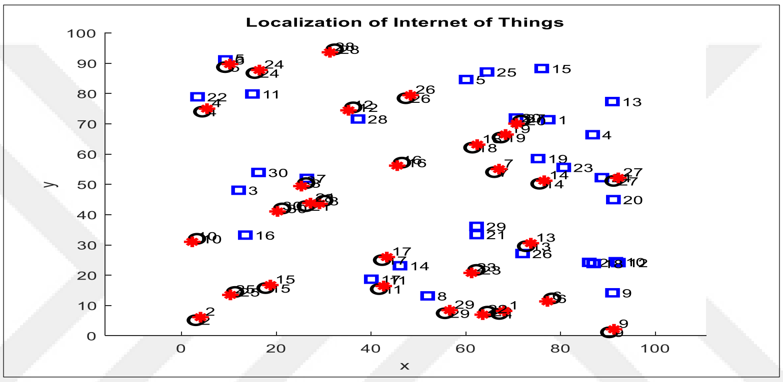

Figure 4.1: Implementation and Simulation Environment of the Proposed Method for IoT Localization

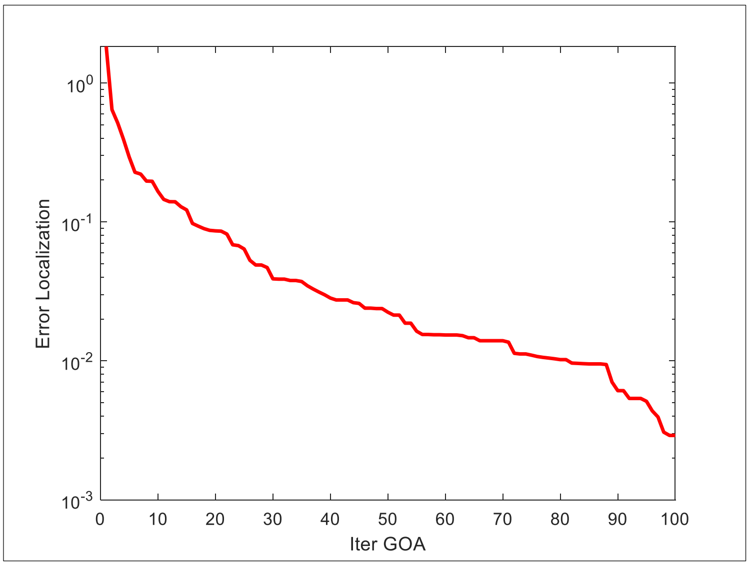

Figure 4.2: Reduction in the Average Localization Error of Smart Objects in the Proposed Method Based on the GOA

As clearly seen, the average localization error decreases as a function of iteration for all objects without GPS. The reduction of localization error based on the GOA iteration shows that:

a. The three-anchor method has a significant error with respect to the distance measurement based on the DV-Hop algorithm. The GOA can be employed to decrease the error.
b. The localization error of objects without GPS significantly decreasing by applying the GOA. The iteration-based error reduction trend confirmed that the GOA is correcting the localization error.

Increasing the number of objects with GPS in the IoT can enhance the quality of localization services in the network because it enables an object without GPS to identify more adjacent objects with GPS.

4.4 ANALYSIS OF TESTS

Equation 4.1 can be employed to evaluate localization errors of objects without GPS in the IoT:

$$E_i = \sqrt{(x_i - x_i')^2 + (y_i - y_i')^2} \tag{4.1}$$

where E_i is the localization error of a sensor node in the actual position (x_i, y_i), which was estimated by the proposed method to be (x_i', y_i'). If n shows the total number of objects without GPS in the IoT, then Eq. 4.2 can be utilized to calculate the average localization of entire objects, which is actually the sum of localization errors divided by the number of network objects:

$$E = \frac{\sum_{i=1}^{n} E_i}{n} = \frac{E_1 + E_2 + \cdots + E_n}{n} \tag{4.2}$$

where E_i is the localization error of the i^{th} smart object, and n shows the total number of objects without GPS in the IoT and E represents the average localization error of these objects. The error is only a test error, and the test can be run for specific times to calculate the localization error in the entire tests on objects without GPS through Eq. 4.3:

$$\bar{E} = \frac{\sum_{i=1}^{Run} E_i}{Run} = \frac{E_1 + E_2 + \cdots + E_{Run}}{Run} \tag{4.3}$$

where *Run* represents the total number of localization tests, and E shows the average localization error of all objects tested in *Run*. Undoubtedly, the IoT localization methods try to minimize $\bar{E}$ as the main localization indicator. For this purpose, the GOA was utilized in the proposed algorithm to reduce the output localization error.

The population size and iteration were assumed to be 5 and 20, respectively, to analyze and evaluate the proposed method and the also the effect of increased number of objects with GPS on the localization errors of the proposed method. The number of objects without GPS was considered constant (30), whereas the number of objects with GPS was assumed to be 10, 20 and 30 to measure the localization errors in 50 different tests. Table 4.2 and Figure 4.3 show the results:

Table 4.2: Comparison of Localization Error in the Proposed Method by Increasing the Number of Objects with GPS

Average Localization Error	Number of Objects with GPS
0.518	10
0.365	20
0.287	30

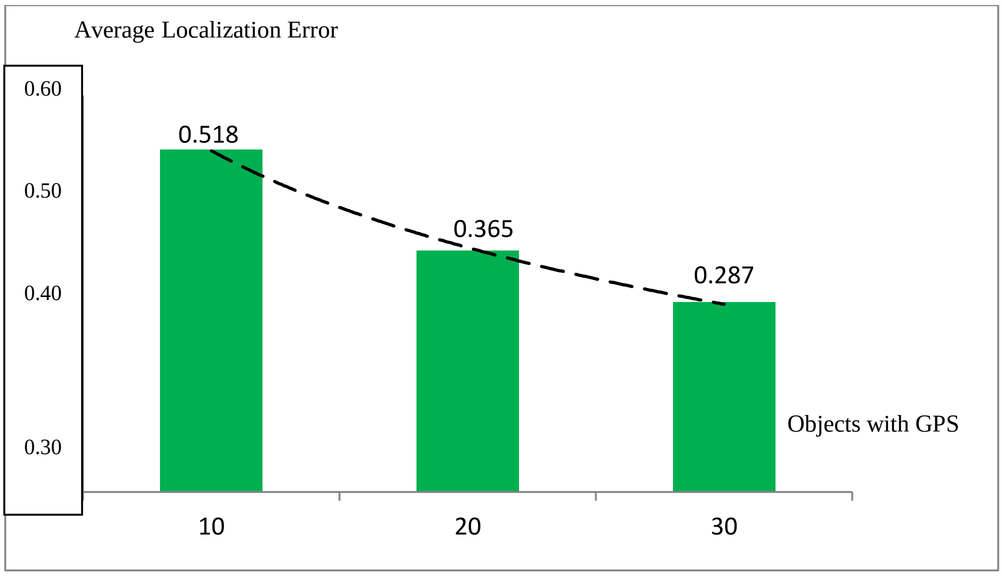

Figure 4.3: Role of Anchor Nodes in Reducing Localization Error in the Proposed Method

According to the test results shown in the above table and figure, the localization error reduced from 0.518 to 0.287 by increasing the number of objects with GPS from 10 to 30 when there were 30 objects without GPS with the population size and iteration of 5 and 20, respectively. In other words, if the number of objects with GPS is tripled, the localization error will decrease 1.804 times because of an improvement in the hop-based distance modeling in the DV-Hop algorithm. At the same time, the effectiveness of the GOA increased by increasing the number of objects with GPS for localization. The density can be considered 10, 20, and 30 to compare the proposed method with the DV-Hop algorithm, regarded as the basic method, by assuming a population size of 10 to run the DV-Hop algorithm. Table 4.3 and Figure 4.4 show the results of comparison:

Table 4.3: Comparing the Proposed Method with the DV-Hop Algorithm in Terms of Localization Error in Different Densities of Objects with GPS

Localization Error of DV-Hop	Localization Error of the Proposed Method	Objects with GPS
0.978	0.518	10
0.892	0.365	20
0.646	0.287	30

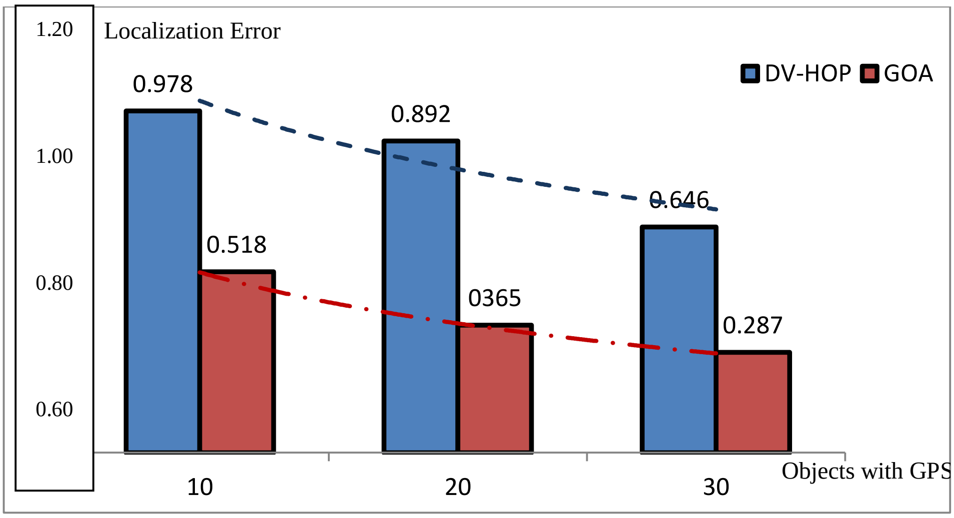

Figure 4.4: Comparing the Proposed Method with the DV-Hop Algorithm in Terms of Localization Error

According to the comparison and analysis of the proposed method and the DV-Hop algorithm in localization error, with increasing the density of objects with GPS from 10 to 30, the localization error of the DV-Hop algorithm decreases from 0.978 to 0.646. However, the localization error of the proposed reduced from 0.518 to 0.287. In fact, the localization error of the DV-hip technique decreased nearly 1.51 times by increasing the number of objects with GPS, whereas it decreased nearly 1.804 times in the proposed method. It is fair to state that the localization error of the proposed method decreased far more than that of the DV-Hop algorithm by increasing the density of objects with GPS.

The proposed method was executed on a Core i5 microprocessor with 4 GB of RAM in MATLAB to evaluate its runtime for different sizes of population. For a more accurate analysis of runtime, it is possible to compare the results with the DV-Hop algorithm and other similar methods such as butterfly optimization algorithm (BOA), particle swarm optimization (PSO) and firefly algorithm (FA) (Arora & Singh, 2017). Table 4.4 and Figure 4.5 show the comparison results. The testing conditions were considered the same so that the proposed method could be compared with other techniques in terms of runtime:

Table 4.4: Comparing the Runtime of the Proposed Method with other Methods

Localization Algorithm	**Localization Algorithm Runtime (s)**
FA	1.940
BOA	0.530
GOA (Proposed)	0.416
PSO	0.490
DV-Hop	0.238

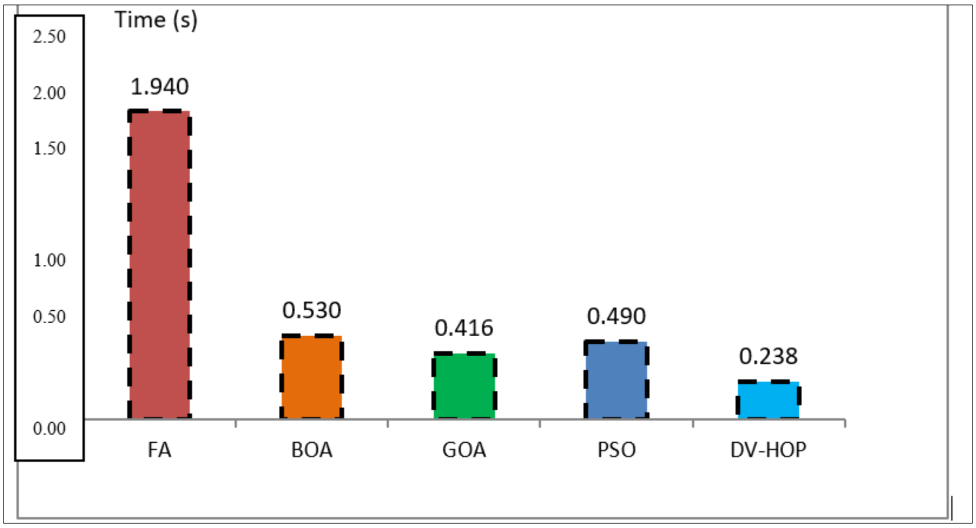

Figure 4.5: Comparing the Proposed Method with other Localization Algorithms in Terms of Runtime

According to the test results, the runtimes of FA, BOA, GOA (proposed method), PSO, and DV-Hop are 1.94, 0.530, 0.416, 0.490, and 0.238, respectively. Therefore, the proposed method has a shorter runtime than FA, PSO, and BOA. However, it requires a longer runtime than the DV-Hop algorithm for localization. The results of analysis show that the runtime of the proposed method is 1.747 times longer than that of the DV-Hop algorithm because of more calculations performed to reduce errors. To evaluate the proposed method (GOA) based on the localization error, it was compared with other localization algorithms such as FA, BOA, PSO and DV-Hop to determine its accuracy for localization. The tests were conducted in the same conditions. Table 4.5 and Figure 4.6 show the comparison results of different algorithms in terms of average localization error of objects with GPS. The conditions were considered the same as the basic paper for the sake of calculations

Table 4.5: Comparing the Proposed Method with other Localization Techniques in Terms f Localization Error

Method	Average Localization Error
FA	0.69
BOA	0.21
DV-Hop	1.439
PSO	0.78
GOA	0.16

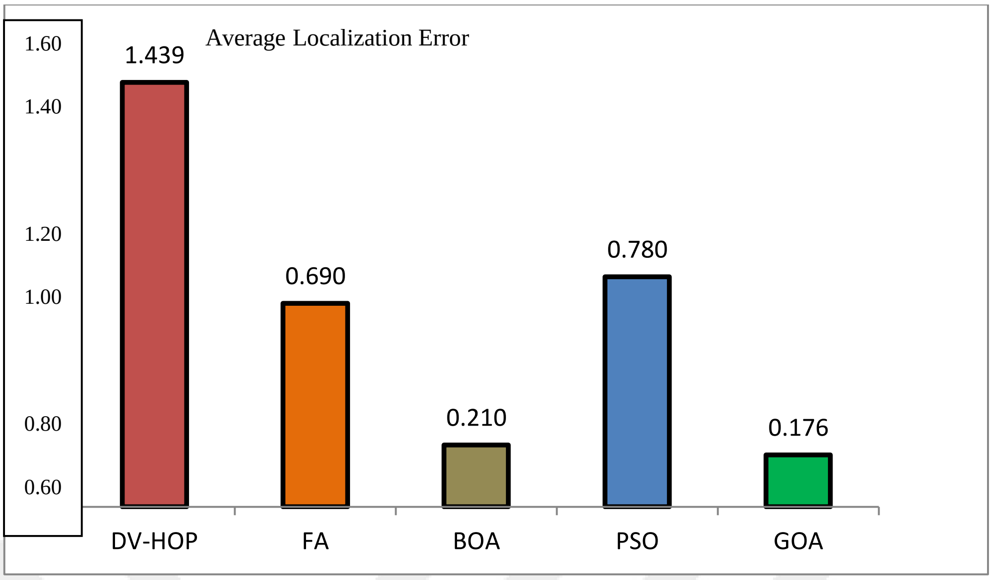

Figure 4.6: Comparing the Proposed Method with other Localization Methods in Terms of Localization Error

According to the test results, the proposed method has a lower localization error in the IoT than FA, BOA, PSO and DV-Hop algorithms. The BOA is ranked second, and the DV-Hop algorithm shows the worst performance.

5. CONCLUSIONS AND FUTURE WORK

5.1 CONCLUSIONS

Localization is a process in which objects without GPS try to determine their positions and locations or those of other objects with GPS. The IoT localization faces specific challenges, and objects should determine their locations and positions very accurately.

In most applications, if objects are unable to calculate their positions and locations accurately, they will be unable to send useful information to the base station because the information is important when its position and location are known in the IoT. At the same time, most routing protocols are useful and practical when the positions and locations of objects are known accurately.

According to the test and implementation results, the localization error of objects without GPS was decreased by applying the GOA in comparison with the DV-Hop and three-anchor methods. The tests also indicated that the reduction of the localization error as a function of the GOA iterations.

This indicates that the proposed algorithm corrected the localization error of the three-anchor method. When the number of objects with GPS was tripled in the proposed method, the localization error decreased 1.804 times. According to the tests, localization error decreased by increasing the population size of the GOA because of an improvement in the DV-Hop modeling.

At the same time, the localization effectiveness of the GOA increased by increasing the number of objects with GPA. The tests also indicated the shorter runtime of the proposed method than the FA, PSO and BOA algorithms.

However, it showed a longer localization runtime than the DV-Hop algorithm. As seen from the results the proposed method has 0.176 for the localization error, while the other methods has high than this value, and this value shows that the proposed method has good performance than other methods. It is hoped that future studies try to develop the proposed method for 3D localization along with other metaheuristic localization algorithms.

5.2 FUTURE WORK

For Future work we can work on the metaheuristic optimization method such as Harris hawks optimization, Genetic Algorithm and gray wolf optimization method to improve the percentage of the accuracy.

REFERENCES

[1] Aktemur, I., Erensoy, K., & Kocyigit, E. "Optimization of Waste Collection in Smart Cities with the use of Evolutionary Algorithms". International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), PP.1-8, 2020.

[2] Al-Safi, H., Munilla, J., & Rahebi, J. ,"Patient privacy in smart cities by blockchain technology and feature selection with Harris Hawks Optimization (HHO) algorithm and machine learning". Multimedia Tools and Applications, PP.1-25, 2022.

[3] Al Hayali, S., Rahebi, J., Ucan, O. N., & Bayat, O. "Increasing energy efficiency in wireless sensor networks using GA-ANFIS to choose a cluster head and assess routing and weighted trusts to demodulate attacker nodes". Foundations of Science,vol.25, no.4, PP.1227-1246, 2020.

[4] Al Shalchi, N. F. A., & Rahebi, J. "Human retinal optic disc detection with grasshopper optimization algorithm". Multimedia Tools and Applications, pp.1-19, 2022.

[5] Alwafi, A. A. W., Rahebi, J., & Farzamnia, A. "A new approach in energy consumption based on genetic algorithm and fuzzy logic for WSN". Proceedings of the 11th National Technical Seminar on Unmanned System Technology 2019, pp.1007-1019, 2021.

[6] Arora, S., & Anand, P. (2021). "Chaotic grasshopper optimization algorithm for global optimization". Neural Computing and Applications, vol.31, no.8,pp. 4385-4405, 2021.

[7] Arora, S., & Singh, S."Node localization in wireless sensor networks using butterfly optimization algorithm". Arabian Journal for Science and Engineering, vol.42,no.8, pp.3325-3335, 2017.

[8] Bae, Y. "Robust localization for robot and IoT using RSSI". *Energies*, vol.*12*,no.11, 2019.

[9] Balico, L. N., Loureiro, A. A. F., Nakamura, E. F., Barreto, R. S., Pazzi, R. W., & Oliveira, H. A. B. F. "Localization prediction in vehicular ad hoc networks". IEEE Communications Surveys & Tutorials, vol.20,no.4, pp.2784-2803,2018.

[10] Bhattacharyya, D. K., & Kalita, J. K. "Network anomaly detection: A machine learning perspective". Chapman and Hall/CRC, 2019.

[11] Bhushan, B., & Sahoo, G. "Requirements, protocols, and security challenges in wireless sensor networks: An industrial perspective". In Handbook of computer networks and cyber security , pp.683-713, 2020.

[12] Buczak, A. L., & Guven, E. "A survey of data mining and machine learning methods for cyber security intrusion detection" . IEEE Communications Surveys & Tutorials,vol.18,no.2, pp.1153-1176, 2015.

[13] Carrez, F."Converged architectural reference model for the IoT", 2013.

[14] Chen, L., Tseng, M., & Lian, X. "Development of foundation models for Internet of Things ". Frontiers of Computer Science in China, vol.4,no.3, pp.376-385, 2010.

[15] Constante Nicolalde, F., Silva, F., Herrera, B., & Pereira, A. "Big data analytics in IOT: challenges, open research issues and tools". World Conference on Information Systems and Technologies, pp.775-788, 2018.

[16] Crichigno, J., Bou-Harb, E., & Ghani, N. "A comprehensive tutorial on science DMZ". IEEE Communications Surveys & Tutorials, vol.21,no.2, pp.2041-2078, 2018.

[17] Cup, K. D. D. http://kdd. ics. uci. edu/databases/kddcup99/kddcup99. html. *The* UCI KDD Archive, 1999.

[18] Dang, L., Yang, H., & Teng, B. "Application of Time-Difference-of-Arrival Localization Method in Impulse System Radar and the Prospect of Application of Impulse System Radar in the Internet of Things". IEEE Access, vol.6, pp.44846-44857,2018.

[19] Darwassh Hanawy Hussein, T., Frikha, M., Ahmed, S., & Rahebi, J. "BA-CNN: Bat Algorithm-Based Convolutional Neural Network Algorithm for Ambulance Vehicle Routing in Smart Cities". Mobile Information Systems, 2022.

[20] Ewees, A. A., Abd Elaziz, M., & Houssein, E. H. "Improved grasshopper optimization algorithm using opposition-based learning". Expert Systems with Applications, pp.156-172,2018.

[21] Friedemann, M., & Floerkemeier, C. "From the Internet of Computers to the Internet of Things". Informatics-Spektrum, vol33,no.2, pp.107-121,2010.

[22] Gumaida, B. F., & Luo, J. "Novel localization algorithm for wireless sensor network based on intelligent water drops". Wireless Networks, vol.25,no.2, pp.597-609,2019.

[23] Hamdani, M., Qamar, U., Butt, W. H., Khalique, F., & Rehman, S. "A comparison of modern localization techniques in wireless sensor networks (WSNs)". Proceedings of the Future Technologies Conference, pp.535-548,2018.

[24] Huang, J., Zhao, Y., Li, X., & Xu, C.-Z. "Ultra-Low Power Localization System Using Mobile Cloud Computing". International Conference on Cloud Computing, pp.1-10,2019.

[25] Jeong, J. P., Yeon, S., Kim, T., Lee, H., Kim, S. M., & Kim, S.-C. "SALA: Smartphone-assisted localization algorithm for positioning indoor IoT devices". Wireless Networks,vol.24,no.1, pp.27-47,2018.

[26] Khelifi, F., Bradai, A., Benslimane, A., Rawat, P., & Atri, M. "A survey of localization systems in internet of things". Mobile Networks and Applications, vol.24,no.3, 761-785,2019.

[27] Khodadadi, F., Dastjerdi, A. V., & Buyya, R. "Internet of things: an overview". Internet of Things, pp.3-27,2016.

[28] Kumar, S. "Performance analysis of RSS-based localization in wireless sensor networks". Wireless Personal Communications, vol.108,no.2, pp.769-783,2019.

[29] Liao, H.-J., Lin, C.-H. R., Lin, Y.-C., & Tung, K.-Y. "Intrusion detection system: A comprehensive review". Journal of Network and Computer Applications, vol.36,no.1,pp.16-24,2013.

[30] Lu, B., Wang, L., Liu, J., Zhou, W., Guo, L., Jeong, M.-H., Wang, S., & Han, G. "Lasa: location aware wireless security access control for IoT systems". Mobile Networks and Applications, vol. 24,no.3, pp.748-760,2019.

[31] Luo, C., Wu, F., Sun, J., & Chen, C. W. "Compressive data gathering for large-scale wireless sensor networks". Proceedings of the 15th Annual International Conference on Mobile Computing and Networking, pp.145-156,2009.

[32] Machine, C. "The Only Coke Machine on the Internet". The Carnegie Mellon University Computer Science Department, 2014.

[33] Mahmud, R., Kotagiri, R., & Buyya, R. "Fog computing: A taxonomy, survey and future directions". In *Internet of everything*,pp. 103-130,2018.

[34] Miraz, M. H., Ali, M., Excell, P. S., & Picking, R."Internet of nano-things, things and everything: future growth trends". Future Internet, vol.10,no.8, pp.68,2018.

[35] Mirjalili, S. Z., Mirjalili, S., Saremi, S., Faris, H., & Aljarah, I. "Grasshopper optimization algorithm for multi-objective optimization problems". Applied Intelligence, vol.*48*,no.4, pp.805-820,2018.

[36] Motta, R. C., de Oliveira, K. M., & Travassos, G. H. "A framework to support the engineering of internet of things software systems". Proceedings of the ACM SIGCHI Symposium on Engineering Interactive Computing Systems, pp1-6,2019.

[37] Moustafa, N., & Slay, J."UNSW-NB15: a comprehensive data set for network intrusion detection systems".UNSW-NB15 network data set. Military Communications and Information Systems Conference (MilCIS), pp.1-6,2015.

[38] Nath, R. K., Bajpai, R., & Thapliyal, H. "IoT based indoor location detection system for smart home environment". IEEE International Conference on Consumer Electronics (ICCE), pp.1-3,2018.

[39] Palermo, F."Internet of Things". Information Week ings done wrong stifles innovation,2017.

[40] Pardini, K., Rodrigues, J. J. P. C., Kozlov, S. A., Kumar, N., & Furtado. "IoT-based solid waste management solutions: a survey". Journal of Sensor and Actuator Networks, vol.8,no.1,2019.

[41] Ramakrishnan, R., Gehrke, J., & Gehrke, J. "Database management systems" . McGraw-Hill New York, vol.3.

[42] Saad, E., Elhosseini, M., & Haikal, A. Y. "Recent achievements in sensor localization algorithms". Alexandria Engineering Journal, vol.57,no.4, pp.4219-4228,2018.

[43] Sadowski, S., & Spachos, P. "Rssi-based indoor localization with the internet of things". IEEE Access, vol.6, pp.30149–30161,2018.

[44] Saeed, N., Celik, A., Al-Naffouri, T. Y., & Alouini, M.-S."Localization of energy harvesting empowered underwater optical wireless sensor networks". IEEE Transactions on Wireless Communications, vol.18,no.5, pp.2652-2663,2019.

[45] Salih, K. O. M., Rashid, T. A., Radovanovic, D., & Bacanin, N."A comprehensive survey on the Internet of Things with the industrial marketplace". Sensors, vol.22,no.3,pp.730,2022.

[46] Saremi, S., Mirjalili, S., & Lewis, A."Grasshopper optimisation algorithm: theory and application". Advances in Engineering Software, vol.105, pp.30-47,2017.

[47] Serketzis, N., Katos, V., Ilioudis, C., Baltatzis, D., & Pangalos, G."Improving forensic triage efficiency through cyber threat intelligence". Future Internet, vol.11,no.7, pp.162,2019.

[48] Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. "Toward generating a new intrusion detection dataset and intrusion traffic characterization". ICISSp, vol.1, pp.108-116.

[49] Shit, R. C., Sharma, S., Puthal, D., James, P., Pradhan, B., van Moorsel, A., Zomaya, A. Y., & Ranjan, R. "Ubiquitous Localization (UbiLoc): A Survey and Taxonomy on Device Free Localization for Smart World". IEEE Communications Surveys & Tutorials,2019.

[50] Singh, D., & Singh, V. P. "Comparative study of various distributed intrusion detection systems for WLAN". Global J. Res. Eng. Electr. Electron. Eng., vol.12,no.6, pp.49-56,2017.

[51] Sotenga, P. Z., Djouani, K., Kurien, A. M., & Mwila, M. M."Indoor localisation of wireless sensor nodes towards internet of things", Procedia Computer Science, vol.109, pp.92-99,2017.

[52] Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A."A detailed analysis of the KDD CUP 99 data set". IEEE Symposium on Computational Intelligence for Security and Defense Applications, pp.1-6,2019.

[53] Vatansever, Z., Brandt-Pearce, M., & Bezzo, N. "Localization in optical wireless sensor networks for IoT applications". IEEE International Conference on Communications (ICC), pp.1-6,2019.

[54] Vorst, T. Van der, Eeckhaute, M. Van, Benlarbi-Delai, A., Sarrazin, J., Quitin, F., Horlin, F., & Doncker, P. De. (2019). Application of polynomial chaos expansions for uncertainty estimation in angle-of-arrival based localization. In Uncertainty Modeling for Engineering Applications ,pp. 103-117,2019.

[55] Wang, H., Wen, Y., Lu, Y., Zhao, D., & Ji, C. "Secure localization algorithms in wireless sensor networks: a review". In Advances in Computer Communication and Computational Sciences ,pp. 543-553,2019.

[56] Wang, P., Xue, F., Li, H., Cui, Z., Xie, L., & Chen, J. "A multi-objective DV-Hop localization algorithm based on NSGA-II in internet of things". Mathematics, vol.7,no.2,pp. 184,2019.

[57] Wu, H., Ding, Z., & Cao, J. "GROLO: realistic range-based localization for mobile IoTs through global rigidity". IEEE Internet of Things Journal, vol.6, no.3, pp.5048-5057.

[58] Yaqoob, I., Hashem, I. A. T., Ahmed, A., Kazmi, S. M. A., & Hong, C. S." Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges". Future Generation Computer System*s*, vol.92, pp.265-275,2019.

[59] Zhang, Y., Zhang, M., & Li, M. "Agricultural Internet of Things". In Sensing, Data Managing, and Control Technologies for Agricultural Systems ,pp. 17-40, 2022.

[60] Zheng, J., Dike, C., Pancari, S., Wang, Y., Giakos, G. C., Elmannai, W., & Wei, B.. "An In-Depth Review on Blockchain Simulators for IoT Environments". Future Internet, vol.14,no.6,pp.182,2022.