AI-Enhanced Intrusion Detection and Cluster Head Selection for Quality of Service (QoS) Optimization in Wireless Sensor Networks

Dr. Niyati Kumari Behera[1], A. Radhika[2], Dr. J. Brindha Merin[3], Dr. R.Akila[4]

[1]Assistant Professor Department of Computer Science and Engineering, B.S. Abdur Rahman Crescent Institute of Science and Technology, Vandalur, Chennai. radhika.a@crescent.education, Orcid: https://orcid.org/0000-0002-9384-2949
[2]Assistant Professor (Senior Grade), Department of Computer Science and Engineering, B.S. Abdur Rahman Crescent Institute of Science and Technology, Vandalur, Chennai. radhika.a@crescent.education, Orcid: https://orcid.org/0000-0001-7959-4830
[3]Assistant Professor (Senior Grade), Department of Computer Science and Engineering, B.S. Abdur Rahman Crescent Institute of Science and Technology, Vandalur, Chennai. brindhamerin@gmail.com, Orcid: https://orcid.org/0000-0001-9736-1061
[4]Assistant Professor (Senior Grade), Department of Computer Science and Engineering, B.S. Abdur Rahman Crescent Institute of Science and Technology, Vandalur, Chennai. rakila@crescent.education, Orcid: https://orcid.org/0000-0003-4000-4535

The widespread relevance of wireless sensor networks (WSN) has made them an active area of research. Quality of service (QoS) considerations in WSN design center around limiting power consumption, increasing network longevity, and bolstering safety. The dynamic nature of a Mobile Ad hoc Network (MANET) makes it vulnerable to issues with both power and safety. Optimization of energy is a difficult problem to solve for most of the already available methods, yet routing protocols do it efficiently. Many issues, such as path maintenance, power consumption, security, reliability, and sudden changes in connection characteristics, arise because of the mobility of nodes in MANETs. Current clustering methods suffer from unreliable communication that wastes the power of nodes due to the fact that the interaction lacking from the model by the possibility of dropped packets. Therefore, improving system QoS necessitates employing energy-efficient communication methods. The network's dependability may be greatly enhanced by deploying the AI – Enhanced Multicast Routing Technology [AI-EMRT]. Multicasting involves sending data packets from a source node to multiple receiving nodes at once. Multicasting is a cost-effective way to send data. QoS criteria including energy, longevity, and security are developed in this research with a novel code for safe unequal clustering using an intrusion detection system. The suggested model begins by selecting the Tentative Cluster Heads (TCHs) via a Dynamic Cognitive Fuzzy Driven Clustering Approach [DCFDCA] with the help of residual energy, BS distance, and neighbor distance are all possible input variables. Finally, a

successful intrusion detection system based on a dense web of convictions is implemented on the Cluster Heads (CH) to detect the invasion of privacy in a cluster-based WSN, ensuring its security. The higher energy efficiency, network lifetime, packet delivery percentage, mean delay, and intrusion detection performance of the proposed approach rate has been shown by an extensive set of experiments.

Keywords: Quality of service , Wireless Sensor Networks, Mobile Ad hoc Network ,AI – Enhanced Multicast Routing Technology, Tentative Cluster Heads, efficiency and Dynamic Cognitive Fuzzy Driven Clustering Approach.

1. Introduction

Due to its versatility and low cost, MANET has emerged as a viable communication medium [1]. Even though MANETs are easy to set up, their primary shortcoming is that battery-operated nodes die when their power supply runs out, which can throw the network out of synchronization [2]. Mobile ad hoc networks (MANETs) are utilized by a wide range of computing solutions, such as portable computers, smartphones, and tablets [3]. Node connections are the most common type of network connection for mobile devices at the present time [4]. The use of mobile devices for communication is now fundamental [5]. MANETs are defined by the presence of a network partition as a part of the overall network topology [6].

In addition to energy efficiency, MANETs must meet stringent standards for data security, especially when dealing with highly confidential information [7]. The MANET can be used for a variety of purposes, including surveillance of wildlife, military operations, disaster relief, scientific research, and "smart agriculture [8]. Most security approaches in use today are computationally intensive, making it difficult to render energy efficiency and security in the network at the same time [9]. Considering the importance of MANETs in applications like surveillance and warfare operations, it is crucial to deal with the security concerns of these networks [10]. Sensitive information is sent between commanding units and the range limit of their communications [11]. As a result, there is a pressing requirement for reliable, low-power protocols [12]. Therefore, it is crucial that routing protocols be created in a way that makes it impossible for typical attacks like data interception, spoofing, and network jamming to succeed [13].

Keeping data secure while being sent across an internetwork is the biggest obstacle. There are security concerns with cloud-based platforms and software. For existing techniques to guarantee the confidentiality, authenticity, and integrity of transmitted data, blockchain technology has been proposed as a secure methodology or mechanism [14]. The potential for data to grow stale as a consequence of greater mobility and diverse topology has prompted worries about disconnection and packet loss across nodes [15]. Many studies have shown that the implementation of routing protocols in MANETs significantly enhances both network safety and efficiency [16]. However, MANET communication protocol development is still a work in progress. Various pieces of software are introduced to verify the functionality of the specified communication protocols [17]. To verify the efficacy of numerous ad hoc network modeling and testing software is the industry standard for analyzing and evaluating communication protocols [18].

The need for the Internet of Things (IoT) has grown over the past few years, necessitating the development of both software and hardware for nodes of sensors to filter and collect data [19]. It additionally possible to observe complicated nodes whose characteristics are carefully regulated to the deployment of diverse detectors able to detecting the data from the surrounding environment [20]. The standard definition of a WSN is a network of dispersed sensors deployed in various locations to collect data about their immediate environment and relay that data to a control node [21]. Clustering sensor nodes, which may achieve the performance in a better manner, is a top-tier approach to save power and money in the Internet of Things. Improving WSN efficiency is hampered by issues with topology, quality of service, and power.

In addition, the optimization of energy resources relies heavily on the optimization of resources in complex systems. Clustering is thought to be the optimal strategy in this case as well. For this reason, several studies have tracked the development of energy optimization via smart clustering models. In most cases, CHs are formulated by clusters once the nodes are grouped together. The CH then collects information from additional nodes in the cluster that aren't CHs. The data is processed and sent to the base station. In IoT-WSN, the CHs send data directly to the BS, cutting down on the amount of energy needed to cover the same distance [22].

The following are the paper's most significant contributions:

- ❖ To boost system QoS, it's important to choose low-power communication protocols. Hence by Incorporating Artificial Intelligence - Enhanced Multicast Routing Technology [AI-EMRT] into a network that has the potential to significantly improve its reliability is proposed in this paper.
- ❖ Here developing a unique secure clustering algorithm that uses an intrusion detection technique to meet certain quality-of-service requirements.
- ❖ Starting with the input parameters, the proposed model uses a Dynamic Cognitive Fuzzy Driven Clustering Approach [DCFDCA] to choose the Tentative Cluster Heads (TCHs).

The following is the sequence in which the sections of this paper are presented: The literature on cluster selection models is reviewed here in the Background research section. In the next section, the originality of the suggested model is described. This example illustrates the objective model taken into account while choosing the best cluster head in an IoT-connected WSN. The achieved results are discussed in the Results and discussions section, and the paper concludes up in the Conclusion section.

2. Background Research:

The authors provide a multi-criteria model for selecting CHs in IoT-based WSNs, taking into account factors like lifetime of the network and node energy consumption.

Suresh Kumar, R et al. [23] proposed the multicast routing protocol [MRP] where it is possible that MANET network reliability can be greatly enhanced. Focusing on multicast routing quality of service (QoS) evaluation is the main objective of this research.

Multicasting involves sending data packets from a source node to many reception nodes simultaneously. Transmittal expenses are lowered by multicasting. One of the difficulties of MANET is choosing a cluster head. This proposed research paper uses optimal route selection (ORS) to choose a cluster leader and a backup leader in case the original leader fails, generate an optimal path between the leader and each member node based on the pair's reliability and each node's energy, and set up the path that it uses the fewest possible hops and the most possible energy. ORS is superior to conventional approaches in providing an energy-efficient channel between the central processing unit and node of a cluster and the member node. The suggested ORSMAN outperforms cutting-edge methods in terms of throughput, latency, jitter, and packet delivery ratio.

Veeraiah, N et al. [24] delivered in this research, by presenting an Optimization Algorithm - based multipath routing protocol [OA-MRP] for use in MANETs. Fuzzy clustering and fuzzy Naive Bayes (fuzzy NB) are two techniques that can be used to pick a cluster head (CH) and detect intrusions, respectively, in a MANET. Then, the Bird swarm-whale optimization algorithm (BSWOA), which is the combination of BSA and WOA, is used as the routing protocol to advance the trusted-node multi-hop routing. Fitness elements including interaction, power, confidence, and throughput are used to choose the best routes. Performance measurements are used to evaluate the methods against assaults like floods, black hole, and selective transmission drop.

Jaaz, Z. A et al. [25] elaborated to ensure effective interaction amongst IoMT-based systems, focused on developing a modeling clustering called Whale optimized weighted fuzzy based cluster head selection method [WOWF-CHS]. Despite the fact that many novel methods are being created to improve IoMT QoS, clusters has come out as the frontrunner due to the energy savings it gives in the medical industry. The current clustering method's biggest flaw is that it uses a communication model that doesn't account for the possibility of packet loss, leading to erratic communication that wastes the power of medical nodes. In terms of quality of service, the experimental investigation demonstrates that the suggested method has merit outperforms its rival approaches. This indicates that the proposed technique not reduces power consumption in 5G-based IoMT systems, improves service quality by ensuring that cluster-head is evenly distributed over the network.

Jubair, M. A et al. [26] demonstrated in this research, we propose a novel routing protocol, QoSC, which combines QoS-aware Cluster Head (CH) selection with hybrid cryptography [QoS-CH]. The QoSC protocol is comprised mostly of two parts: QoS-based CH selection and hybrid cryptography. Strengthening the network's foundation and connections during data transmission, the CH selection module uses QoS factors to choose nodes. During the network's communication process, the firmness and connectivity are enhanced by module for choosing CHs based on quality of service. The QoSC protocol is tested with an NS2-based VANET simulator. The simulator includes three models: an assault model, a load model, and a model of the network itself. A variety of scenarios, including attacks via wormholes and gray holes, are modeled in the simulator.

Alazab, M et al. [27] elaborated this work presents a novel method for choosing CHs, which makes use of a tweaked version of the Rider Optimization Algorithm (ROA). The suggested algorithm divides the answers into two groups, the best and the second-best, depending on

the fitness value. Fitness Averaged-ROA (FA-ROA) is used to update the first set based on the mean value of cyclists who are being bypassed and riders who are being followed, respectively. The suggested FA-ROA may be proven effective through comparison with other cutting-edge optimization models, specifically with regards to the number of surviving nodes and the normalized energy. Many objectives, such as the removal of delay and the preservation of a consistent energy consumption rate, would be made possible by applying an approach to clustering to the intra-distance inter-distance between the CH and the nodes. To select the best CH, it is necessary to optimize for factors like latency, power consumption, and network distance among other things in IoT devices.

Maheswari, M et al. [28] incorporated the suggested model begins by selecting the tentative cluster heads (TCHs) by adaptive neural fuzzy based clustering [ANFC] with the help of three input parameters: residual energy, distance to base stations (BS), and length to neighbors. Deer hunting optimization (DHO) is then used to have the TCHs compete for the finest possible CHs. Considering factors like entropy, proximity to base station, degree, centrality of nodes, and quality of connections, the DHO based clustering algorithm computes a fitness function. The proposed solution makes use of load balancing during the cluster maintenance period to further enhance performance. Finally, a deep belief network-based intrusion detection system is run on the CHs to detect the existence of network intruders, a crucial step toward ensuring the safety of a cluster-based WSN.

Existing methods named MRP, OA-MRP, WOWF-CHS, QoS-CH, ROA, and ANFC are a few examples of frequently employed model techniques that may benefit from some fine-tuning. In this research, we suggest implementing AI-EMRT, or Artificial Intelligence Enhanced Multicast Routing Technology, into a network to dramatically increase its reliability, security and energy.

3. Artificial Intelligence Enhanced Multicast Routing Technology: [AI-EMRT]

Security is an unusual example of a QoS (Quality of Service) attribute, and a lack of adequate protection against unwanted access to a network will result in a violation of the QoS restrictions. Because of the ever-changing nature of MANET topologies, routing in these systems is crucial. The environmental sensing, monitoring, and other activities performed by mobile nodes are the root cause of these types of mobile networks. In addition, the propensity of networks to broadcast leads to security vulnerabilities. The development of security-aware routing algorithms is fundamental due to the insecure nature of the physical route of communication. Effective security services for mobile users are provided by MANETs, and these include accessibility, availability, Integrity, Privacy, and authenticity.

The process of cluster creation is complicated and fraught with difficulties. The choice of CH is critical in minimizing total energy use. In order to fix the issues with lowering energy usage and expanding the lifespan of networks, AI-EMRT is proposed. Specifically, we propose AI-EMRT, an IoT-specific multi-objective cluster head choice optimization model. This strategy ensures energy efficiency by factoring in the CHs option nodes, residual power ratio, and energy balance degree. Selecting a CH for a WSN-IoT network requires formulating a multi-objective function that takes into account temperature, load distance,

latency, and energy. The primary goal of this proposal is to minimize the total load, the total temperature, the total delay, and the total distance between all possible nodes, while simultaneously maximizing the normalized energy that remains in each node.

$$RC = (E + 1) - \sin\ (M)\% \int \ln (MN) \quad (1)$$

In equation (1), RC stands for root cause, E for environmental sensing, M for monitoring, MN for mobile nodes, log for mapping, and sin for group identification using trigonometry.

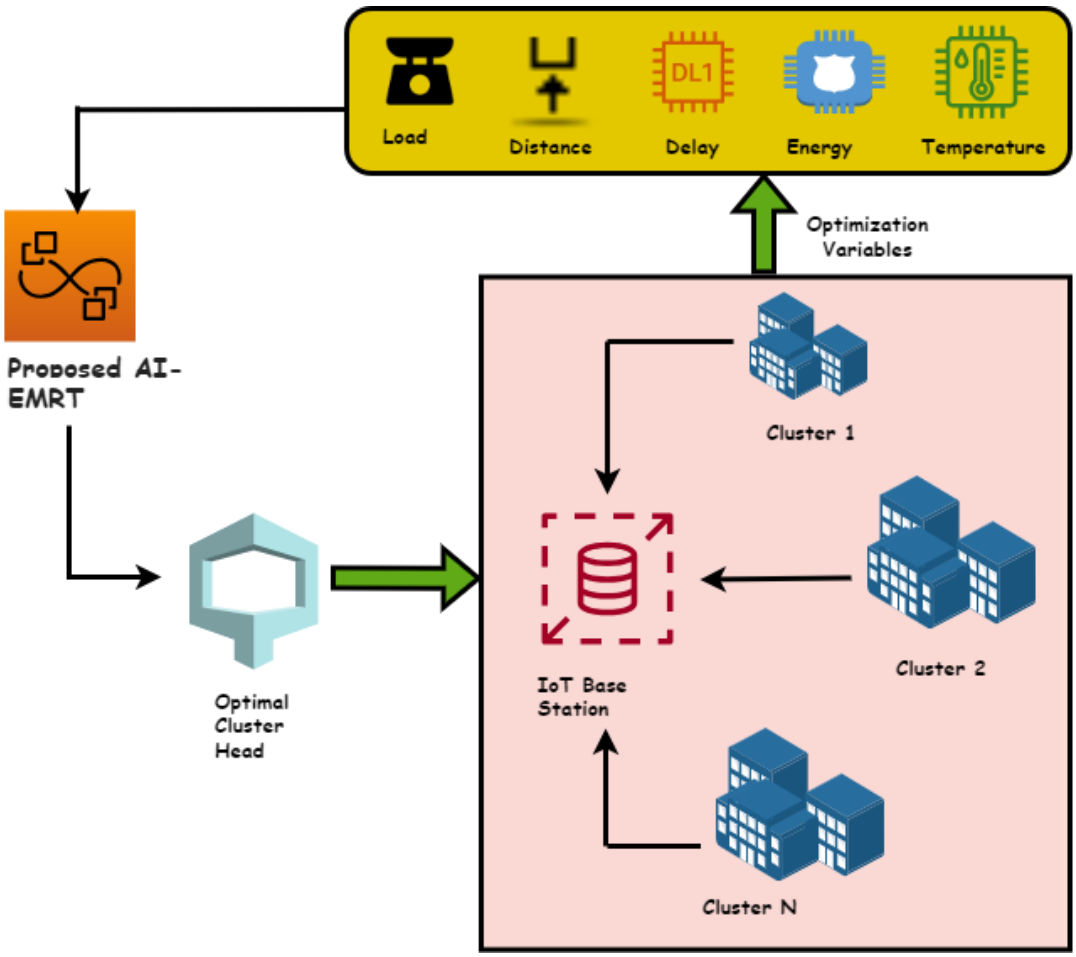

Figure 1. Interpretation of CH Selection Model

Latency, distance, and energy are used to determine the WSN's CH which is depicted in figure 1 as shown. There are always a lot of problems that need fixing before IoT can run more efficiently and use less energy. Temperature and load considerations are taken into account with the addition of WSN to IoT devices. Typically, a WSN's number of clusters is dynamic, and CHs are selected at random from among the network's nodes. As mentioned before, in WSN, the choice of CH is based on performance measures like nodes' separation, delay, and residual energy. As a result, CHs are allowed direct communication with the BS, while all other nodes are forbidden from doing so. The selection of a CH in a WSN-IoT

system is made more difficult by the inclusion of network information from both types of networks. As a result, we create a multi-objective function by considering factors such as temperature, load, energy, distance, and latency between nodes. Our proposed method, AI-EMRT, will be used to resolve this multi-objective problem.

$$G = (L + T + B + D) \times \int \cos^{-1}(B) \frac{NE}{D-1} \quad (2)$$

The expression (2) represents G as a primary goal, where is a mathematical function for the group and is a mathematical function for total distance, delay, temperature and load and NE denotes the normalized energy.

$$CH = \frac{\sqrt{n(o)} - \int(\sqrt{s+re}) \times \sum d}{G} \quad (3)$$

CH denotes the cluster head, $n(o)$ denotes the node separation delay, s denotes the separation, re denotes the residual energy and d denotes the distance and these are the variables in equation (3).

$$CH = \frac{\sqrt{n(o)} - \int(\sqrt{s+re}) \times \sum d}{L+T+B+D) \times \int \cos^{-1}(B) \frac{NE}{D-1}} \quad (4)$$

When equation (2) is substituted into equation (3), the cluster head is represented by equation (4).

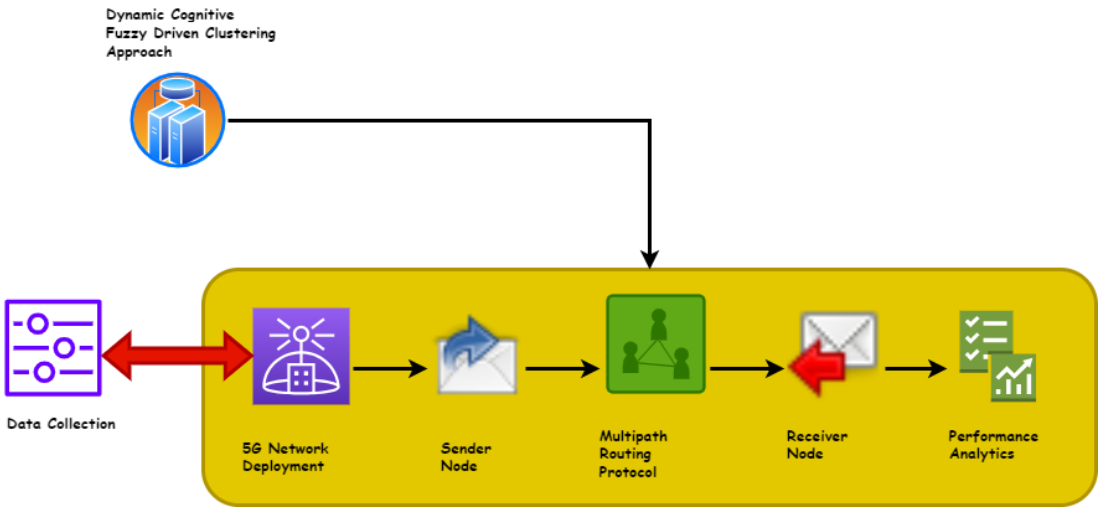

Figure 2. General Progression for the Proposed Work

This part describes the general progression of the proposed method. Figure 2 shows both sender and receiver nodes and processes like data collecting, DCFDCA, and a low-overhead multi-path routing protocol which are depicted in the schematics of a proposed method. Datasets with missing values are not a problem for the suggested filtering and normalization procedures. The method can avoid the use of less-than-ideal solutions in order to find the best one. These advantages make it possible to use the method as-is to a wide variety of restricted and unrestrained optimization problems that arise in real-world contexts. When

using a weighted fuzzy-based clustering, the contribution of such clusters is neutralized because the relevant weights would be close to 0 or equal to zero. In D2D communications, it is challenging to develop a low-overhead multi-hop routing strategy that meets a wide range of performance criteria. Base stations (BS) play a supporting role in the pathfinding procedure. In this way, the BS will not be overworked, and the route-finding process will consume as little network bandwidth as possible. The base station (or cellular 5G cellular infrastructure) is responsible for keeping track of all active D2D (device- to-device) sessions and the routing information for each one. As a result of the route discovery process, the most up-to-date route must be persisted at a dependable and robust network node, such as the BS. By modifying traditional dynamic source routing (DSR) for 5G to incorporate D2D communication, we can simplify and reduce the complexity of route discovery and route management. There have been no significant changes to DSR. Limits the number of network-wide broadcasts of route requests. Using the network's resources efficiently during route discovery is essential and finally the nodes communicate each other through the proposed approach and performance is noted.

$$R_t = F * \left(T_e(\mathrm{Btm}), T_d(\mathrm{Btm}), T_q(\mathrm{Btm})\right) + S_t$$

From the above-stated equation (5) where S_t be the sender signal , R_t be the receiver signal, F be the frequency of the node taken for consideration $T_e(t)d(t)$, and $T_q(t)$ are trusted nodes, service providers of energy, Qos, detection , and surroundings all have a limited amount of trustworthiness in this field will be either [0 or 1], and Btm is broadcasted time.

$$R_t = \frac{\iint T_e(\mathrm{Btm}) * T_d(\mathrm{Btm}) * T_q(\mathrm{Btm})}{S_t}$$

Progress in the development of one's core cross-values $T_q(\mathrm{btm})$ listed from the above equation (5) are usedin the equation given aboveequation (6);The initial service request processing time and the cross-selling phase processing time are exponentially distributed with different parameters are used.

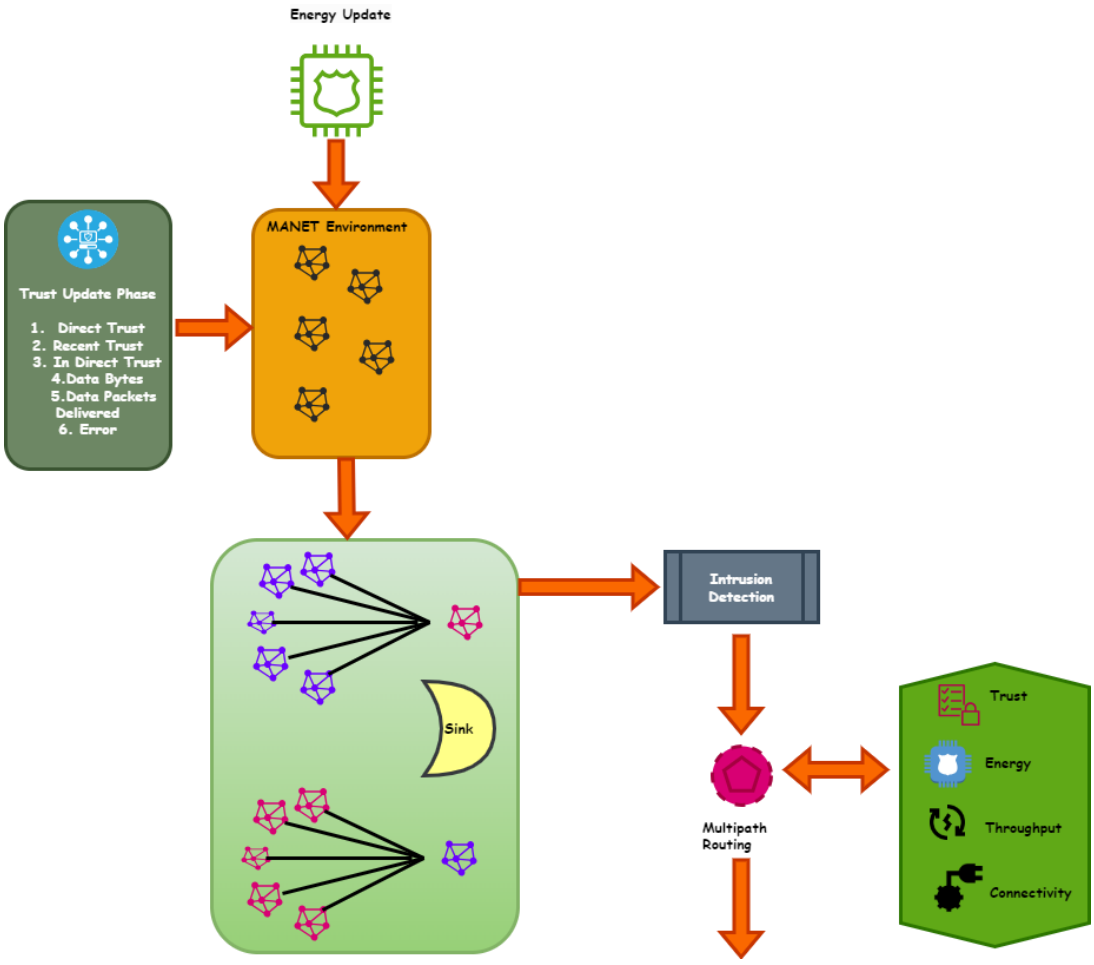

Figure 3. Multipath Routing Scheme for MANET

The process flow for the proposed multipath routing is shown in Figure 3. Because of the current energy crisis, the nodes in a MANET are organized into clusters using one of several different clustering techniques. In addition, the malicious nodes are identified, and secure communication inside the network is guaranteed, by assessing the nodes' security factors. After the network has been set up, in a trust table, the degree of confidence in each node is recorded and maintained hence that nodes with high enough trust factors can communicate with one another. Fuzzy clustering is then used to choose the CH after the trust table has been built. Path establishment is performed using trustworthy CHs, and then multipath selection is performed using the resulting optimization.

$$\sum T = T_{DT} + T_{IDT} + T_R + T_{DB} + T_{DP} + T_{ER} \quad (7)$$

The above equation (7) shows that the T represents the Trusted phase of the node, T_{DT} be the direct trust, T_{IDT} be the indirect trust, T_R be the recent trust, T_{DB} be the data bytes, T_{DP} be the data packets delivered and T_{ER} be the error rate.

$$\frac{dT_o}{dt} = \emptyset + \left(1 - \left(\frac{e^{\beta tm} - e^{-\beta tm}}{e^{\beta tm} + e^{-\beta tm}}\right)^2\right) - \log(T)$$

To demonstrate this, consider equation (8), where is the dependent variable for $\frac{e^{\beta tm} - e^{-\beta tm}}{e^{\beta tm} + e^{-\beta tm}}$ and its resolution, which is discussed in equation where $\frac{dT_o}{dt}$ become a hyperbolic gradient that is reversed with the value of $e^{\beta tm}$.Not that, the derived function reveals that trust $e^{\beta tm}$does not steadily increase during the trust-building stage.

$$\frac{dT_o}{dt} = \emptyset + \left(1 - \left(\frac{e^{\beta tm} - e^{-\beta tm}}{e^{\beta tm} + e^{-\beta tm}}\right)^2\right) - \log(T_{DT} + T_{IDT} + T_R + T_{DB} + T_{DP} + T_{ER})$$

(9)

As a result, it is clear from statement (8) that trust values increase over time.

Hence by solving equation (7) in equation (8) we get the above equation (9) as shown above.

To prevent misunderstandings, trust is essential in a MANET, as trustworthy nodes are allowed to send and receive messages. As a result, the network's transmission and reception are activated according to the nodes' relative degrees of trust, which is calculated and tabulated for all n nodes. Direct trust (DT), indirect trust (IDT), recent trust (RT), trust based on data bytes (DB), error, and DP delivery are the six trust criteria that follow. In advance, the nodes create a trust table and its starting value is 1. Intrusion detection in MANET is guaranteed to work before any multi-path connection is established by consulting the trust table of the nodes.

In this research, fuzzy clustering is used to group the MANET nodes together that the network's overall energy efficiency can be maximized. Selecting the best possible CH in a network that all subsequent communications can proceed through that CH is the ultimate goal of clustering. The most suitable CH is chosen using an empirical criterion: trust. In the fuzzy clustering process, nodes are classified into clusters according to how similar they are to one another, known as the membership degree. Therefore, fuzzy clustering helps with the efficient administration of overlapping data, and, depending on the membership function of the nodes, a node can correspond to more than one cluster.

The theory is that nodes with the closest distance to the CH should be clustered together. Thus, the cluster hubs (CHs) are first initialized at random during the clustering process. The new CH is then calculated based on the membership function, which is the result of computing membership values for each node with regard to its CH in step two. New CHs are derived by repeating the process a set number of times. It's worth noting that the sink node utilizes the trust factors of the nodes in the network to detect intruders, using information conveyed to the sink from other nodes (or cluster members) via CHs when calculating the optimal CHs. Once the invader is identified, the compromised node is cut off from the network. The basic objective of intrusion detection is to ensure a safe connection to a network without compromising speed or incurring unneeded delays. A node is assigned to a category based on the highest class probability calculated from the trustworthiness of its constituent nodes. This prevents the unauthorized nodes from exchanging data with the network and allows the authentic nodes to proceed with the optimal multipath selection.

$$T_C = ((1 - PB) * (1 - PF_P) * (1 - PD_P)) \quad (10)$$

T_C is the probability of a successful transmission over the channel, PB is the probability of a packet being blocked, PF_P is the probability of a failed transmission over the channel, and PD_P is the probability of a packet being discarded after an infinite number of retries in the above equation (10).

The first stage in ensuring a safe transmission in a MANET network is intrusion detection, which selects the authentic nodes in such a way that they form a communication link among the source and destination nodes. Effective communication is ensured by selecting the optimal way using an optimization technique that takes into account factors such as trust, energy, throughput, and connection of the nodes in the path.

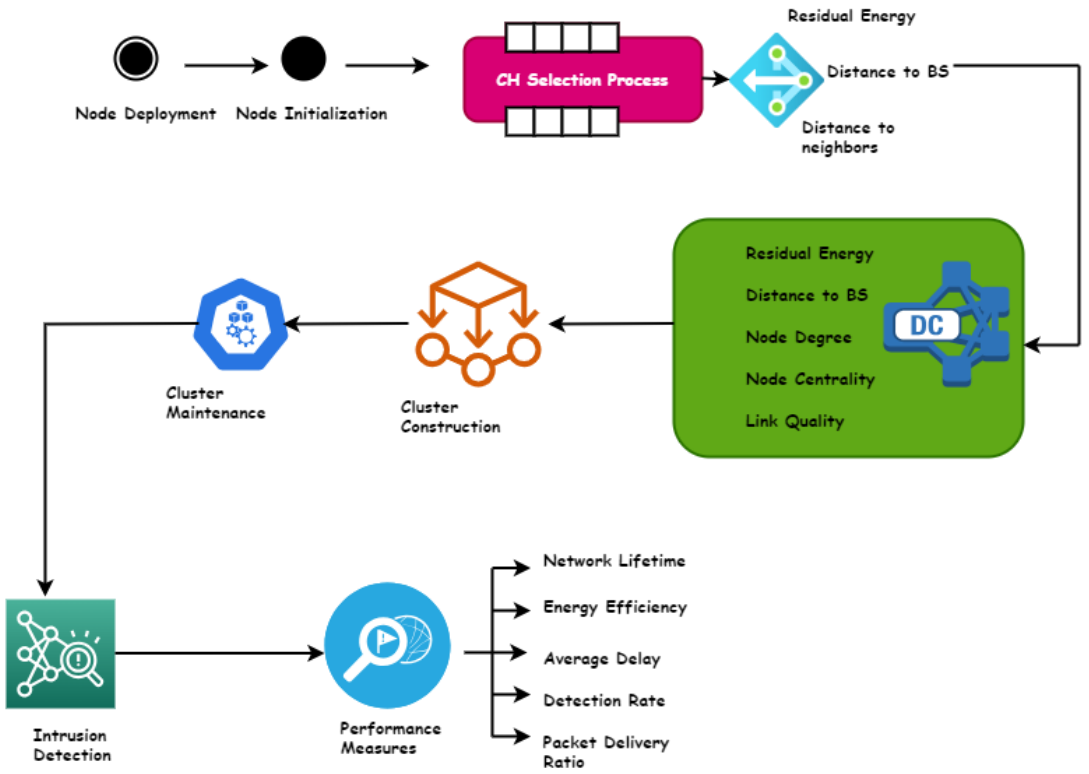

Figure 4. Cluster Head Selection Process

Figure 4 depicts the basic idea behind the provided AI-EMRT model. After the nodes are distributed at random, the network is initialized by gathering neighbor data. The BS then uses the fuzzy method to select an initial group of TCHs. The fitness function (FF) is then used to choose the FCHs, which is the next step in the clustering procedure. The CHs closest to BS likely to deplete its energy after repeated use. When this occurs, we enter the cluster maintenance phase to ensure that all nodes are carrying their fair share of the work. When all else fails, it's time to launch the intrusion detection procedure and find out who's been snooping around our network.

$$E_{TR} = \frac{CF\ (\ SP*\ (CE_{Tx})) - RP*(CE_{Rx})}{CF\ (A*\ (CE_A)} \quad (11)$$

As shown in Equation (11), cognitive elements filter each transmission roundE_{TR}, and bandwidth is greatly achieved; SP provides an estimate of the total number of packets sent; RP provides an estimate of the number of packets received based on size; a stands for aggregation; and P stands for packets and CF be the cognitive frequency.

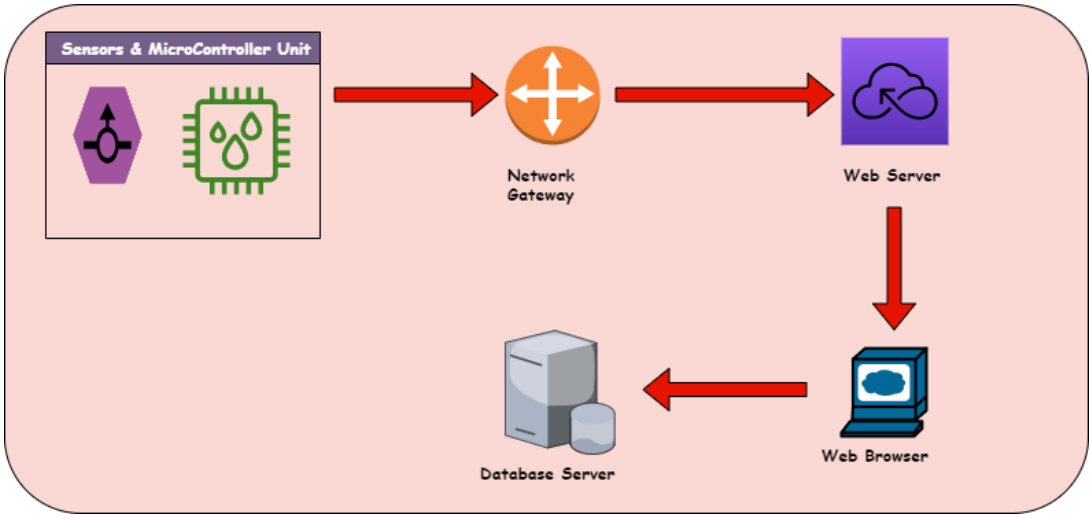

Figure 5. Synthesis of an Intelligent EMRT Framework

In terms of reliability and productivity, the proposed architecture is shown to perform better in experiments than competing designs. Therefore, the proposed AI-EMRT not lowers the energy consumption of edge-based devices equally spreads CHs over the system to extend its life span. Figure 5 depicts the overall system framework where the data is sensed and controlled by sensor & microcontroller unit. From here the data is transmitted through network gateway and is send across web server then to web browser and finally it stores in database server.

In this research, we use intrusion detection in the Internet of Things to illustrate how AI - Enhanced Multicast Routing Technology [AI-EMRT] may be applied to the research of security protocols in the IoT. Throughput, packet delivery ratio, bandwidth, power consumption, and lifetime security were all measured and verified.

4. Results & Discussion:

It has been proposed to improve data protection, routing, and security without using the longest way by implementing AI - Enhanced Multicast Routing Technology [AI-EMRT]. The proposed AI-EMRT technique has been evaluated with the help of this simulation analysis software. To compare the section's defenses to those of other modern models like MRP, OA-MRP, WOWF-CHS, QoS-CH, ROA, and ANFC, refer to the accompanying bar chart. A total of 145 forms were discovered, each with five qualities and four classes. The

procedures for this project's sampling are detailed in Table 1.

Routing protocols and their security can be evaluated using this method based on an IoT approach. For this research, user relied on data provided by a commercial source. Table 1 displays the complete data set.

Tabulation 1: Data set

S.No	Data	Description
1.	Number of Samples	10,20,30,40,50
2.	For users	10,20,30,…90
3.	Taken into account	70
4.	Samples of instructional material	70%
5.	Preliminary testing	75%

4.1 Packet Delivery Analysis:

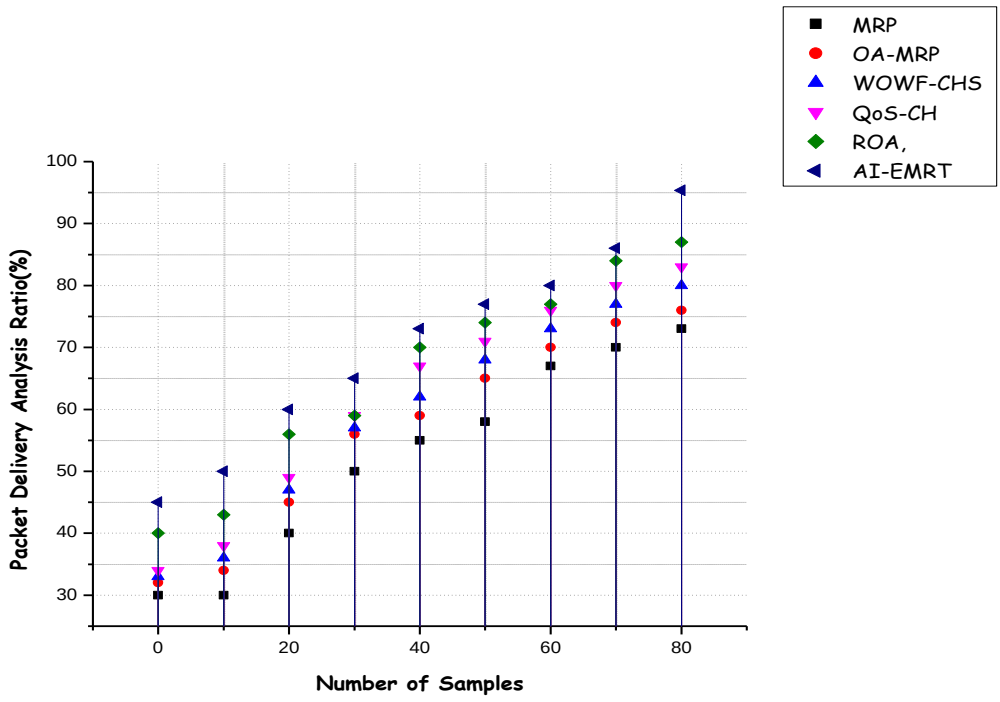

Figure 6. Packet Delivery Analysis

The above-described Packet delivery analysis ratio is used to examine the data. In Figure 6, the percentage of successfully delivered packets is displayed against the number of samples

along the x-axis. When compared to sending fewer packets at a slower rate, sending more packets in a shorter amount of time yields better results. The packets must arrive at the destination within a certain time window for the transmission technique to be successful. All other approaches fail in comparison to the suggested AI-EMRT model.

4.2 Throughput Analysis:

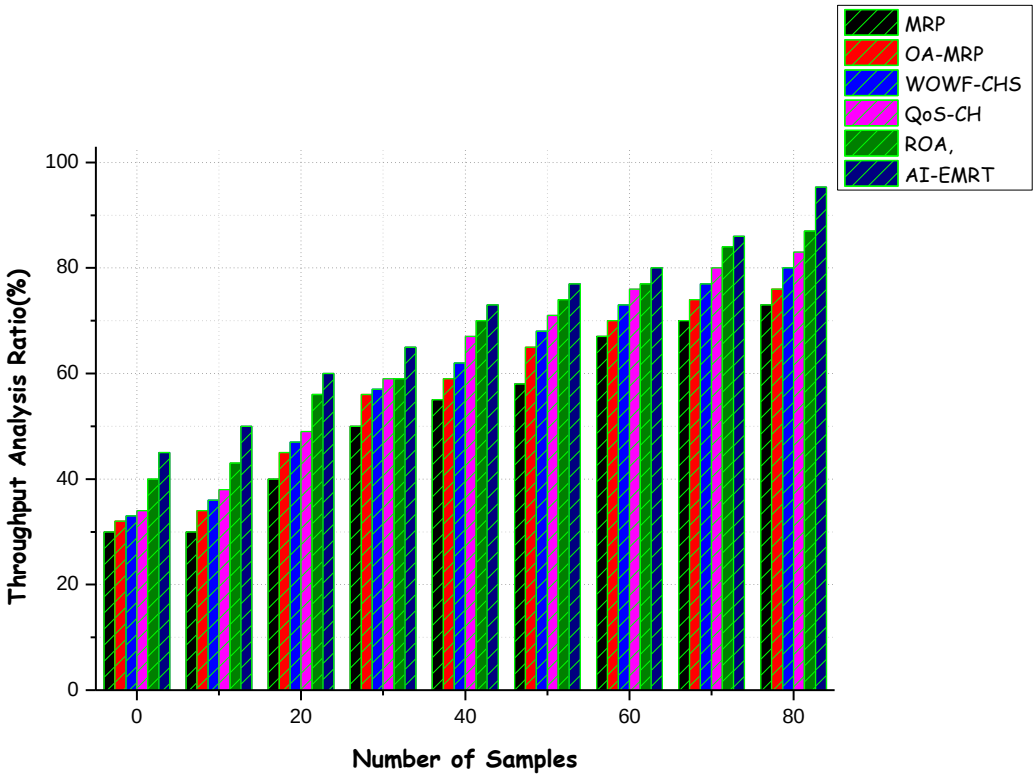

Figure 7. Throughput Analysis

The aforementioned Throughput Analysis Ratio is used for the analysis of the results. Figure 7 shows a scatterplot of throughput analysis ratio (y-axis) versus sample size (x-axis). The AI-EMRT model proposes a path across the node that is superior to those given by other methods. Therefore, the model is efficient since the path must reach its destination as quickly and accurately as possible.

4.3 Energy Consumption Analysis:

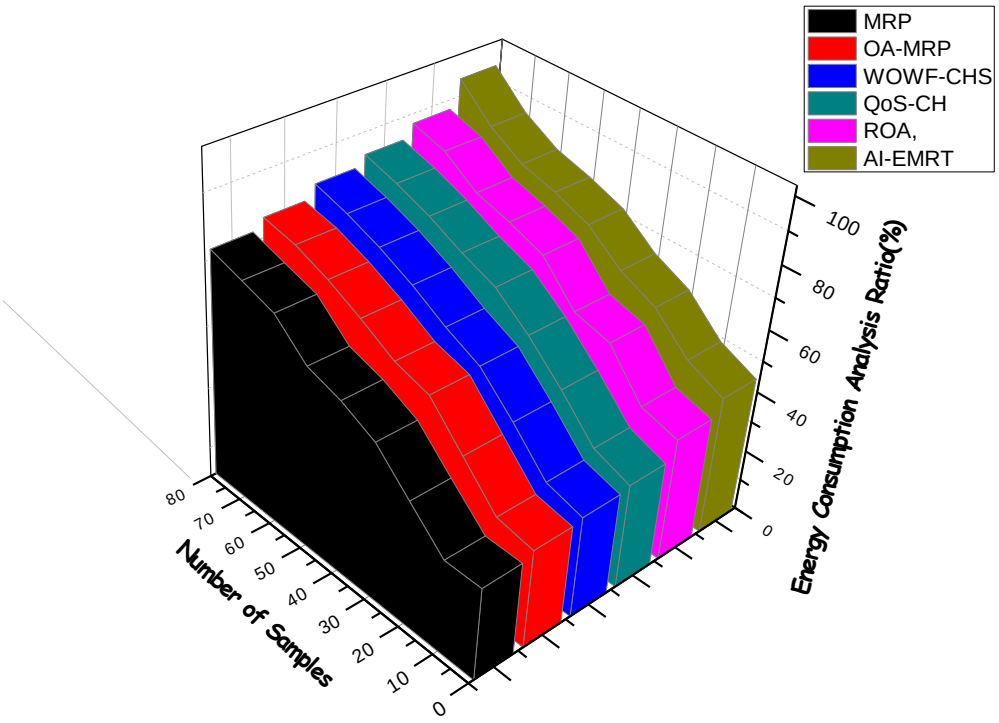

Figure 8. Energy Consumption Analysis

This led us to employ the ratio for analyzing energy consumption presented above in our examination of the data. In Figure 8, the y-axis shows the percentage of total energy used and the x-axis shows the total number of samples. The efficiency of a system increases as its energy consumption decreases. The AI-EMRT model outperforms every other available treatment option.

4.4 Security Analysis:

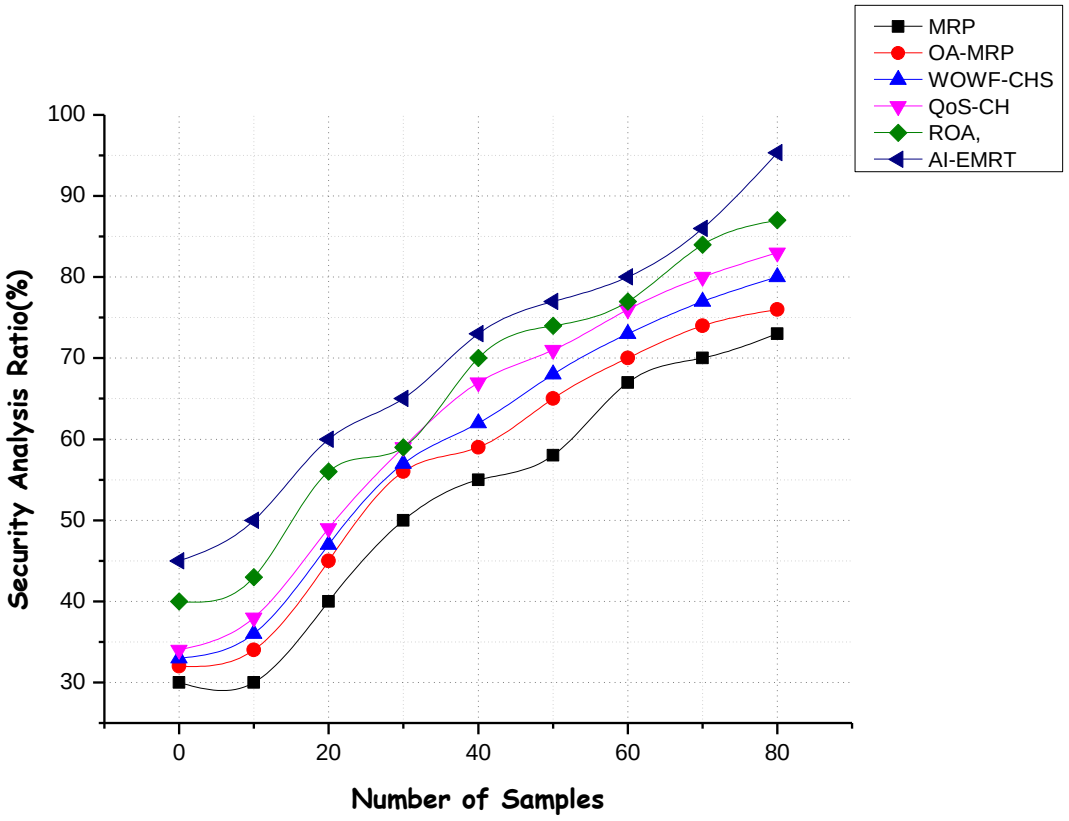

Figure 9. Security Analysis

Figure 9 show that the use of security analysis ratios has no bearing on the reliability of the samples. When compared to other methods already in use, AI-EMRT achieves a higher level of security when transmitting data. In order to prevent data degradation caused by infiltration, it is crucial that the data be transmitted via a network with minimal noise. Data transmission security is improved upon over what is currently available.

4.5 Intrusion Detection Analysis:

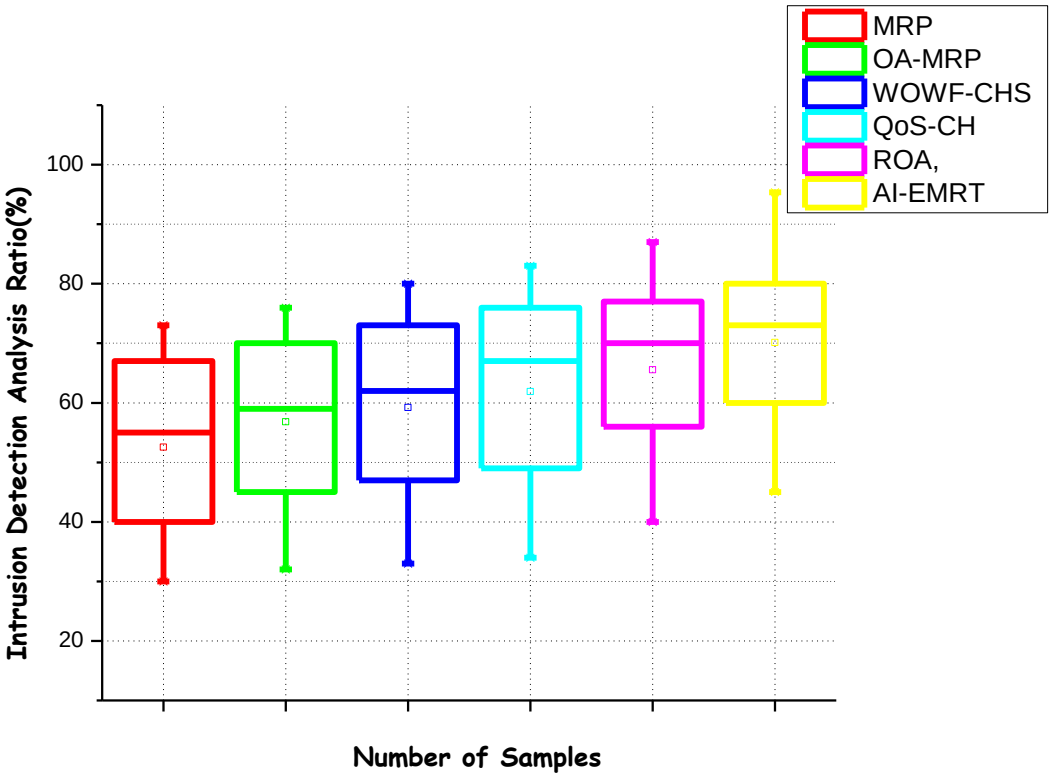

Figure 10. Intrusion Detection Analysis

The aforesaid ratio is used as the analysis basis for intrusion detection. Figure 10 depicts intrusion detection analysis by displaying the number of samples against their intrusion detection analysis ratio. The effectiveness of the channel as a whole decreases whenever a packet is sent, making simultaneous transmission preferable. Data can be sent over greater distances using this method long as more packets are sent. All other approaches fail in comparison to the suggested AI-EMRT model.

With respect to the aforementioned metrics, AI-EMRT outperforms the currently-available MRP, OA-MRP, WOWF-CHS, QoS-CH, ROA, and ANFC. This paper claims that improvements to data security and efficiency are being made through advancements in intrusion detection and service quality in response to the aforementioned competition.

5. Conclusion:

Users assessed IoT routing strategies for their ability to reduce operating costs, time delays, and total energy consumption under demanding operational settings and severe energy limitations. Users have presented a novel method of using sensor networks called AI-EMRT

for selecting cluster heads. It has been discovered that AI-EMRT can significantly reduce energy consumption. AI-EMRT's capabilities in Ad Hoc networks were compared to the cognitive routing progress made by Ad Hoc networks. Data delivery success rates can be improved by as much as 50 percent over existing models. A multicast network's reliability, throughput, and output can all benefit from an improved multicast routingmethod. Mesh-based multicasting is utilized to reduce control overheads and maximize bandwidth utilization without increasing energy consumption or network latency. The approach could be enhanced by taking into account additional matrices, such as trust reputation and communication load, while choosing the cluster leader. If you want to know how long a network will last or how many nodes it can support, you can conduct more simulation at a certain time. The algorithm's adaptability makes it useful for MANET and wireless sensors. Consequently, the proposed method Secure and dependable packet delivery is ensured by taking into consideration trusted nodes along the path. The simulated system performs at its best if the control overhead is kept to a minimum. Thus, the proposed technique of wireless network routing surpassed the other existing model by 95.4 percentage points in terms of efficiency.

References

1. Nguyen, D. C., Cheng, P., Ding, M., Lopez-Perez, D., Pathirana, P. N., Li, J., ... & Poor, H. V. (2020). Enabling AI in future wireless networks: A data life cycle perspective. IEEE Communications Surveys & Tutorials, 23(1), 553-595.
2. Morales-Molina, C. D., Hernandez-Suarez, A., Sanchez-Perez, G., Toscano-Medina, L. K., Perez-Meana, H., Olivares-Mercado, J., ... & Garcia-Villalba, L. J. (2021). A dense neural network approach for detecting clone id attacks on the rpl protocol of the iot. Sensors, 21(9), 3173.
3. Protogerou, A., Kopsacheilis, E. V., Mpatziakas, A., Papachristou, K., Theodorou, T. I., Papadopoulos, S., ... & Tzovaras, D. (2022). Time Series Network Data Enabling Distributed Intelligence—A Holistic IoT Security Platform Solution. Electronics, 11(4), 529.
4. Gill, S. S., Xu, M., Ottaviani, C., Patros, P., Bahsoon, R., Shaghaghi, A., ... & Uhlig, S. (2022). AI for next generation computing: Emerging trends and future directions. Internet of Things, 19, 100514.
5. Wang, L., Liu, Z., Liu, A., & Tao, F. (2021). Artificial intelligence in product lifecycle management. The International Journal of Advanced Manufacturing Technology, 114, 771-796.
6. Salh, A., Audah, L., Shah, N. S. M., Alhammadi, A., Abdullah, Q., Kim, Y. H., ... & Almohammedi, A. A. (2021). A survey on deep learning for ultra-reliable and low-latency communications challenges on 6G wireless systems. IEEE Access, 9, 55098-55131.
7. Nguyen, D. C., Cheng, P., Ding, M., Lopez-Perez, D., Pathirana, P. N., Li, J., ... & Poor, H. V. (2020). Wireless AI: Enabling an AI-governed data life cycle. arXiv preprint arXiv:2003.00866.
8. Hou, X., Wang, J., Fang, Z., Zhang, X., Song, S., Zhang, X., & Ren, Y. (2021). Machine-learning-aided mission-critical Internet of Underwater Things. IEEE Network, 35(4), 160-166.
9. Zafar, S., Ahad, M. A., Ali, S. I., Mehta, D., & Alam, M. A. Smart and Sustainable Approaches for Optimizing Performance of Wireless Networks.

10. Tang, B., Shah, V. K., Marojevic, V., & Reed, J. H. (2023). AI Testing Framework for Next-G O-RAN Networks: Requirements, Design, and Research Opportunities. IEEE Wireless Communications, 30(1), 70-77.
11. Zafar, S., Ahad, M. A., Ali, S. I., Mehta, D., & Alam, M. A. (Eds.). (2022). Smart and Sustainable Approaches for Optimizing Performance of Wireless Networks: Real-time Applications. John Wiley & Sons.
12. Senevirathna, T., La, V. H., Marchal, S., Siniarski, B., Liyanage, M., & Wang, S. (2022). A survey on XAI for beyond 5G security: technical aspects, use cases, challenges and research directions. arXiv preprint arXiv:2204.12822.
13. Ambika, N. (2022). An Augmented Edge Architecture for AI-IoT Services Deployment in the Modern Era. In Handbook of Research on Technical, Privacy, and Security Challenges in a Modern World (pp. 286-302). IGI Global.
14. Vermesan, O., Coppola, M., Nava, M. D., Capra, A., Kornaros, G., Bahr, R., ... & McGrath, S. (2020). New waves of IoT technologies research–transcending intelligence and senses at the edge to create multi experience environments. Internet of Things–The Call of the Edge. Everything Intelligent Everywhere.
15. Filho, C. P., Marques Jr, E., Chang, V., Dos Santos, L., Bernardini, F., Pires, P. F., ... & Delicato, F. C. (2022). A systematic literature review on distributed machine learning in edge computing. Sensors, 22(7), 2665.
16. Essah, R., Tetteh, A., Baidoo, P. K., Duah, B., & Teye, E. Q. (2021). Information Processing in IoT Based Manufacturing Monitoring System. International Journal of Research in Engineering, Science and Management, 4(8), 168-177.
17. De Alwis, C., Kalla, A., Pham, Q. V., Kumar, P., Dev, K., Hwang, W. J., & Liyanage, M. (2021). Survey on 6G frontiers: Trends, applications, requirements, technologies and future research. IEEE Open Journal of the Communications Society, 2, 836-886.
18. Mansour, M., Gamal, A., Ahmed, A. I., Said, L. A., Elbaz, A., Herencsar, N., & Soltan, A. (2023). Internet of Things: A Comprehensive Overview on Protocols, Architectures, Technologies, Simulation Tools, and Future Directions. Energies, 16(8), 3465.
19. Kar, B., Yahya, W., Lin, Y. D., & Ali, A. (2023). Offloading using traditional optimization and machine learning in federated cloud-edge-fog systems: A survey. IEEE Communications Surveys & Tutorials.
20. Alnajar, O., & Barnawi, A. (2023). Tactile internet of federated things: Toward fine-grained design of FL-based architecture to meet TIoT demands. Computer Networks, 231, 109712.
21. Yadav, S. (2021). SD-WAN Service Analysis, Solution, and its Applications.
22. Wong, E., Mondal, S., & Ruan, L. (2023). Machine learning enhanced next-generation optical access networks—challenges and emerging solutions [Invited Tutorial]. Journal of Optical Communications and Networking, 15(2), A49-A62.
23. Suresh Kumar, R., Manimegalai, P., Raj, V., Dhanagopal, R., & Johnson Santhosh, A. (2022). Cluster Head Selection and Energy Efficient Multicast Routing Protocol-Based Optimal Route Selection for Mobile Ad Hoc Networks. Wireless Communications and Mobile Computing, 2022.
24. Veeraiah, N., & Krishna, B. T. (2020). An approach for optimal-secure multi-path routing and intrusion detection in MANET. Evolutionary Intelligence, 1-15.
25. Jaaz, Z. A., Ansari, M. D., JosephNg, P. S., & Gheni, H. M. (2022). Optimization technique based on cluster head selection algorithm for 5G-enabled IoMT smart healthcare framework for industry. Paladyn, Journal of Behavioral Robotics, 13(1), 99-109.
26. Jubair, M. A., Mostafa, S. A., Zebari, D. A., Hariz, H. M., Abdulsattar, N. F., Hassan, M. H., ... & Alouane, M. T. H. (2022). A QoS aware cluster head selection and hybrid cryptography routing protocol for enhancing efficiency and security of VANETs. IEEE

Access, 10, 124792-124804.
27. Alazab, M., Lakshmanna, K., Reddy, T., Pham, Q. V., & Maddikunta, P. K. R. (2021). Multi-objective cluster head selection using fitness averaged rider optimization algorithm for IoT networks in smart cities. Sustainable Energy Technologies and Assessments, 43, 100973.
28. Maheswari, M., & Karthika, R. A. (2021). A novel QoS based secure unequal clustering protocol with intrusion detection system in wireless sensor networks. Wireless Personal Communications, 118, 1535-1557.