Study on the Performance of Manet Using Parameter Optimization and Automatic Updating of the Routing Information

Sonia[1], Dr. Banita[2]
[1]*Scholar, BMU,Rohtak*
[2]*Professor, BMU, Rohtak*

Abstract: Mobile networking refers to the technology that allows data and speech to be sent between specific mobile network nodes through the use of wireless media and radio spectrum transmission. In general, the term "mobile" refers to devices that are intended to be carried by their users and are hence portable and lightweight. In this piece of research, we presented a hybrid version of the swarm optimization model as a means of enhancing the MANET routing protocols. The MANET networks will have their settings optimised thanks to the optimization that was presented. Particle Swarm Optimization (PSO) and Cat Swarm Optimization have been merged into the model that has been proposed (CSO). This research will establish a technique that can be applied to the revealing of MANT networks, also known as mobile sensor networks. The study will also investigate improved mechanism(s) that can be utilised to prevent degraded routing concerns in order to improve performance. The results that are obtained by using the suggested model are considered to be the best results when compared with PSO and CSO.

keywords: MANET, optimization, routing

INTRODUCTION

It is possible for nodes in a wireless ad hoc network, also known as a MANET, to connect with one another in order to send and receive messages in a network that is self-configuring and does not require any infrastructure. Due to the fact that the nodes in such a network are autonomous and free to move in any direction, as well as enter or exit the network at any moment, it is feasible to construct topologies that are exceptionally dynamic. MANETs may be distinguished from other types of wireless networks by their decentralised organisational structure. In a traditional network, messages are transmitted and received by nodes through their interaction with a central base station. These networks have not seen any significant shifts as of recently. On the other hand, MANETs make it possible for nodes to move about freely and to form temporary links with other nodes. The proliferation of internet use and wireless network connectivity has led to an increase in interest in MANETs, which in turn has led to their increased use. Due to the absence of infrastructure in a number of fields, including environmental monitoring, military communications, and disaster aid, ad hoc networks have become increasingly popular. It has been proven that constructing a hierarchy helps increase scalability in MANETs, which is important because the dynamic nature of MANETs makes efficient routing difficult. Clustering is a common approach utilised in the routing process. In the past, we had developed a method that picks cluster heads on the basis of connectivity, battery power, and packet loss rate. Training the parameters that were used in the earlier procedure is the primary focus of the work that we are doing here.

MANETs are significantly more successful than other sorts of dispersed threats because they concentrate on the application layer of the protocol stack rather than the network or data connection layers. This gives them an advantage over other types of dispersed attacks. In order for each packet to get at its final destination in the shortest amount of time, it must first go via a large number of nodes that serve as intermediaries. Failure to comply to the standards established by the routing protocol might make a victim vulnerable during the detection or maintenance phase of a malicious routing assault. Recent research has uncovered that Byzantine, wormhole, and blackhole (or sinkhole) attacks can be very complex and covert forms of routing assaults. Utilizing an intrusion detection system (also known as an IDS) to determine where assaults are coming from in a MANET is currently one of the most fiercely disputed subjects in MANET security. In light of the arguments presented above, MANET ought to have an intrusion detection system set up as a secondary layer of defence as soon as possible.

Utilizing intrusion detection systems allows for the identification and investigation of computer intrusions (IDS). An IDS system would often have components such as methods for modelling and identifying aberrant behaviour as well as sophisticated procedures. They make an effort to investigate and determine whether or not the network is being exploited for malicious reasons. The most typical method for accomplishing this involves collecting data from a wide variety of systems and networks and analysing it to look for potential vulnerabilities. Traditional intrusion detection and prevention measures like as firewalls, access restrictions, and encryption have their limitations when it comes to defending networks and systems against more complex attacks such as denial of service attacks (DoS). A great many of the systems that are built on these methodologies are plagued by substantial rates of false positive detection, in addition to a lack of ongoing adaptation to new and emerging hazardous behaviours. As a consequence of this, machine learning makes it easier for security professionals to locate and patch flaws in computer systems by making data summarization and visualisation easier to do. In order to improve detection rates and flexibility, many Machine Learning (ML) methodologies have been applied to the problem of intrusion detection. They are typically utilised in order to maintain accurate and up-to-date records of the attack in its entirety.

Over the course of the last several years, network security has become an increasingly important issue for discussion in both academic circles and the business world. Network interruption and assault have become more significant hazards for users of data networks as the size and dispersion of the data network continues to increase, and this is especially true for wireless data networks that are still in the process of being developed. There are many different kinds of intrusions that may be made into wireless networks, ranging from unobtrusive listening in to disruptive interference. Large-scale mobile networks are very expected to face intermittent disruptions at some point over the course of several years. This is due to the fact that it is famously difficult to protect wireless systems from being attacked. MANET networks, which stand for Mobile Ad-hoc Network, are especially susceptible to the security flaws that are typical of wireless networks. In a MANET, mobile clients are responsible for constructing the network topology for correspondents operating within a specific radio frequency range. The data can be sent by the nodes of an ad hoc network using any type of wireless or multi-hop routing. The safety of these networks is in jeopardy, which indicates that the protection of the consumer is also in jeopardy. Within the scope of this thesis is an investigation of the Trust-Based paradigm of Non-Cryptographic MANET Security. The logical realities present a difficult challenge for ad hoc system management when it comes to data security. Because they are the first thing that must be taken into account, wireless networks are more susceptible to attacks such as passive eavesdropping and active interference. These attacks can be carried out in a number of different ways. To begin, there is a dearth of trustworthy third-party certification authority (TTPs), which makes it difficult to effectively deploy security measures online. This makes appropriate deployment of security measures online extremely difficult. Because of this, mobile devices are now more susceptible to denial-of-service assaults (DoS), and it becomes more difficult to execute algorithms that need massive calculations, such as public key algorithms. MANETs are susceptible to attacks from both insiders and outsiders, with the former being more challenging to identify than the latter. As a result, in order to ensure the security of networks, it is essential to be vigilant regarding both forms of intrusions. In conclusion, the nomadic character of nodes in an Ad-hoc network creates a greater opportunity for assaults. This is because the capacity to reconfigure the network is severely constrained in such a network. It is difficult, for instance, to differentiate between routing data that has become obsolete or has expired and fraudulent routing data.

RECENT TRENDS IN QoS

QoS Enhancement Approaches

This section addresses all of the many tactics and aspects that can have an effect on the quality of service provided by MANETs. There are multiple approaches in MANETs on which work has been done to improve QoS. The goal of routing algorithms is to get the best possible results by optimising for factors including route, jitter, power consumption, and cross-layer routing. Parameter optimization is feasible because to the fact that models and architecture have an impact on the overall performance of the MANET. Models utilise techniques that are founded on the concept of resource over-provisioning. In order to improve

performance, some algorithms and cross-layer designs are being created as part of other models that are based on learning algorithms, artificial intelligence, and machine learning that are now under development.

QoS Routing Algorithms: The route was selected specifically to produce the lowest BER at the terminating node. Wherever the mobile nodes disperse and fall out of range, a serious issue with QoS occurs. Due to the increased mobility of nodes, a proper solution is necessary to resolve this QoS deviation issue. The primary goal of routing algorithms is to optimise factors like as jitter, power consumption, and cross-layer route latency in order to improve QoS.

2. Architecture supporting QoS

Additionally, models and architectures have been established to enable QoS. These models and architectures have been developed to improve MANET performance. In MANETs, a proper model and well-organized design may provide QoS.

Insignia: It is an IP-based system named INSIGNIA that provides QoS support for signalling inside the context of an Internet Protocol. It is used to overprovision needed resources for MANETs in order to improve QoS performance.

FQMM: FQMM (Flexible Quality of Models for MANETs) is presented in 2000 as a way to improve the quality of service (QoS) in MANETs. It is often used to improve QoS through the properties of network models, namely the INTSERV and DIFFSERV QoS models.

WARN Model:The use of SWARN for overall traffic analysis improves the QoS of any ad hoc network. Here, sender-based admission control is used to regulate the transmission of specific data through UDP or User Datagram Protocol. The increased QoS provided by this approach is referred to as soft QoS since it applies to mobile nodes in such a way that real-time sessions may be refused and re-admitted.

3. QoS Using Congestion Control

Using priority as a parameter, the queuing strategy assisted in lowering congestion. The output demonstrates how congestion affects the overall performance of the MANET.

4. Parametric Approach

Mono Criteria Approach: The mathematical model for selecting the QoS is created to examine the many elements, such as mono-criteria and multi-criteria, and these equations may be utilised to aid in the parameter selection process for optimising the outcomes.

Multi Criteria Approach: In this scenario, the model is comprised of four criteria: energy, delay, bandwidth, and packet loss rate.

5. Learning Algorithms

Numerous machine learning algorithms have been applied in the present circumstance to produce a model and sustainable quality of service solutions. All machine-learning algorithms, such as unsupervised, supervised, and reinforcement learning, may be considered learning algorithms. However, some neural network principles contribute significantly to the definition of probabilistic approximations and stochastic computations. SWARM intelligence and ant colony algorithms are two sophisticated implementations of learning algorithms that have been directly employed to improve MANET performance and QoS.

OBJECTIVE

1. To enhance the performance of the MANET using parameter optimization and automatically updating of the routing information using learning algorithms on the nodes.
2. To compare the results with selected learning algorithm and prove that learning algorithms enhance and optimize results

Research Method

This section is broken up into four different primary subsections. In Section 3.1, the PSO algorithm and its general step-by-step approach are presented for the first time. In Section 3.2, the LAR protocol structure and its guiding principles are laid forth. Sections 3.3 and 3.4, respectively, detail the RREQ mechanism and the optimization mechanism, respectively.

Particle Swarm Optimization

The PSO takes into account one form of the P-Metaheuristic Optimization algorithm, which gets its inspiration from creatures that are sociable and live in groups. According to Lü et al. (2014), one of the characteristics that sets PSO apart from other P-

Metaheuristic algorithms is the use of a straightforward mathematical model that has a limited number of optimization equations. When it comes to the searching process, the PSO focuses on two primary parameters: velocity and location (candidate solution). The technological procedure that differentiates PSO from other metaheuristic algorithms is that each particle possesses two candidate solutions: its present solution (position), as well as its best local solution pbest (Mohamed Ali et al., 2021). The exploration ability of PSO is increased because to the presence of two solutions inside the same particle. The particles collaborate in order to obtain the Gbest global best solution. The new location of the particle in the PSO pool may be calculated using Equation (1).

$$x_i^d(t+1) = V_i^d(t+1) + x_i^d(t)$$

Where: $xid(t+1)$ is the new position of the particle, $xid(t)$ is the specified current position of the particle, $Vid(t+1)$ is a new velocity function.

The Equation (2) uses calculate the new velocity of the particle at optimization iteration t+1.

$$V_i^d(t+1) = w(t) * V_i^d(t) + c_1 r_1 \left(pbest_i^d - x_i^d(t)\right) + c_2 r_2 \left(gbest^d - x_i^d(t)\right) \quad (2)$$

Where: both value of $(r1,r2)$is a random value, the constants values $(c1,c2)$ are set value (1.25) according to (Al-saeedi, 2016; Mirjalili & Lewis, 2013), The $Vid(t)$ is velocity of the particle at iteration t, $w(t)$ weight inertia at iteration (t).

Cat Swarm Optimization (CSO)

The Cat Swarm Optimization, often known as CSO, is an algorithm for swarm optimization that was first introduced in. It encourages the cat to behave in a find-and-beat manner. Tracing mode and searching mode are the two pillars on which the CSO algorithm is built technically (Ahmed et al., 2020). In CSO, the cat has a total of three value places, in addition to a flag and a cost value. In most cases, the location of the cat may be considered a candidate solution to the optimization issue with a diminution that is equal to the problem. The accuracy or fitness value that the cat uses to determine the cost value is the cost value. The mode of the flag is either seeking or tracing, and it is designated as the cat. According to the equation, the Seeking Mode will be used (3).

$$P_i = \frac{|FS_i - FS_b|}{FS_{max} - FS_{min}}, \text{ where } 0 < i < j$$

In the tracking mode the cat updated the velocity and position. The cat update it velocity (vk,d) according to equation (4) (chuan Chu et al., 2006).

$$v_{k,d} = v_{k,d} + r_1 \times c_1 \times \left(x_{best,d} - x_{k,d}\right), \text{where } d = 1,2,\dots,M \quad (4)$$

$x$best,d is the position of the cat, that has the best fitness in the cat pool; $x_{k,d}$is the position of cat k . $c_1$is a constant and r1 is a random value in the range of [0,1]

According to equation (4), the cat will now be located at the new coordinates (xk,d).

$$x_{k,d} = x_{k,d} + v_{k,d}$$

Due to the fact that CSO stores the best answer until it reaches the conclusion of the iterations, the ultimate solution will be the cat that has the best position overall.

Ad Hoc On-Demand Distance Vector (ADOV)

MANET and other types of mobile networks can utilise ADSV, which is a reactive routing technology. It has numerous useful properties that make it appropriate for usage in MANET networks, such as dynamic, self-starting multi-hop routing between mobile nodes that seek to construct and maintain an ad hoc network. In addition, it can support a large number of hops without the need for manual configuration. AODV allows for the creation of routes to specific destinations and does not require nodes to maintain these routes when they are not actively communicating with one another. This eliminates the problem of "counting to infinity" and allows AODV to avoid the problem altogether by using objective sequence numbers. This ensures that there are no loops in AODV. In the AODV routing protocol, the routing messages do not contain information about the entirety of the route path across the network; rather, they just contain information about the source and the destination. Within the MANET network, the broadcasts of a route request (RREQ) packet are illustrated in Figure 1.

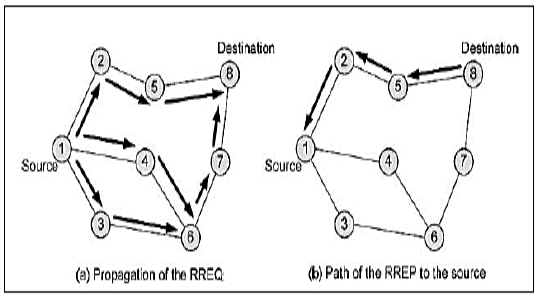

Figure 1 AODV broadcast RREQ

Dynamic Source Routing (DSR)

DSR is a routing protocol that governs the path that packets take via a MANET from their point of origin to their final destination. It gives nodes the ability to dynamically identify a source route over numerous network hops to any destination node of their choosing The DSR routing protocol is primarily comprised of many phases, the most important of which are route discovery and route maintenance. When mobile hosts participating in the DSR protocol wish to send packets, they are required to check their route cache in order to determine whether or not they already have a route to the desired destination. If the network contains a path that leads from the origin to the destination, then a packet will be transmitted to the host It is the responsibility of the host node to initiate route discovery by sending a route request packet that includes the address of the destination along with the address of the source mobile host as well as a unique identification number. This is done in the event that the host node does not have a route, the route does not exist, or the route has not yet reached its expiration date. As a result, the nodes in the network make use of the DSR routing protocol whenever they receive a packet. This ensures that each node can determine whether or not a route to the destination exists If it does not, it appends its address to the packet's route record and then sends the packet along with its routing connections. If it does not, it does not do either There are two scenarios in which a route for a packet is generated: the first is when the request reaches its final destination, and the second is when the cache of an intermediate node includes an active route to the final destination. The data packet that was successfully delivered using DSR routing across the MANET network is seen in Figure 4.

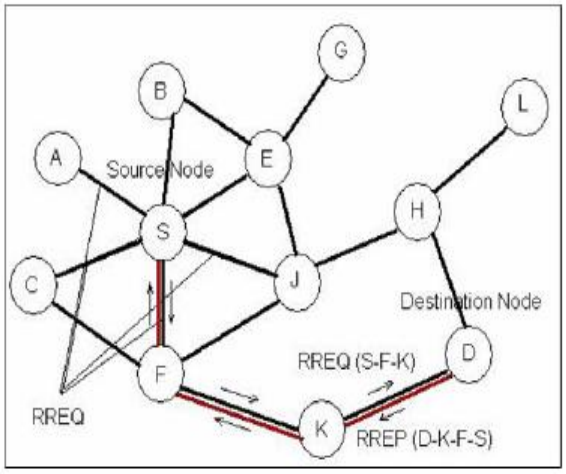

Figure 2 DSR broadcast RREQ

Proposed Hybrid Cat and Particle Swarm Optimization (CPSO)

DSR is a routing protocol that governs MANET packet paths. Nodes may dynamically discover a source route over numerous network hops to any destination node (Al-Dhief et al., 2018). Route discovery and route management make up the DSR routing protocol. When DSR mobile hosts deliver packets, they check their route cache to see if they have a route to the destination. If a route exists from source to destination, a packet is forwarded to the host (Daas & Chikhi, 2018; Mustafa et al., 2020). If the host node doesn't have a route, the route doesn't exist, or the route hasn't expired, it sends a route request packet with the destination address, the source mobile host address, and a unique identification number. When receiving a packet, each node uses the DSR routing protocol to determine if a route exists to the destination (Al-Dhief et al., 2018; Nghi et al., 2019). If not, it adds its address to the packet's route record and sends it with its routing connections (Ahmad et al., 2020). A packet's route is created when the request reaches the destination and when the intermediate node cache has an unexpired route to the destination (Ilyas, 2003). Figure 4 shows a DSR-routed MANET packet delivery.

A. Initialization of the proposed model is mainly based on determining the size of the random population. A random population starts with a size specified by the user and a certain dimension according to the optimization problem.

B. In this step, the proposed system allows the COA to start searching for the first local optimum. If the search stagnates, the system automatically switches

to the PSO search process. The best solution is to switch to the PSO only.

C. If the PSO falls within the local optimum and there is no improvement in the candidate solution, the system automatically switches the search process to COS with the current best solution found by the PSO. When switching, the system lets the swarm optimization algorithms keep their parameters (population, speed) and changes only the best solution.

Figure 3 illustrates the steps of proposed system

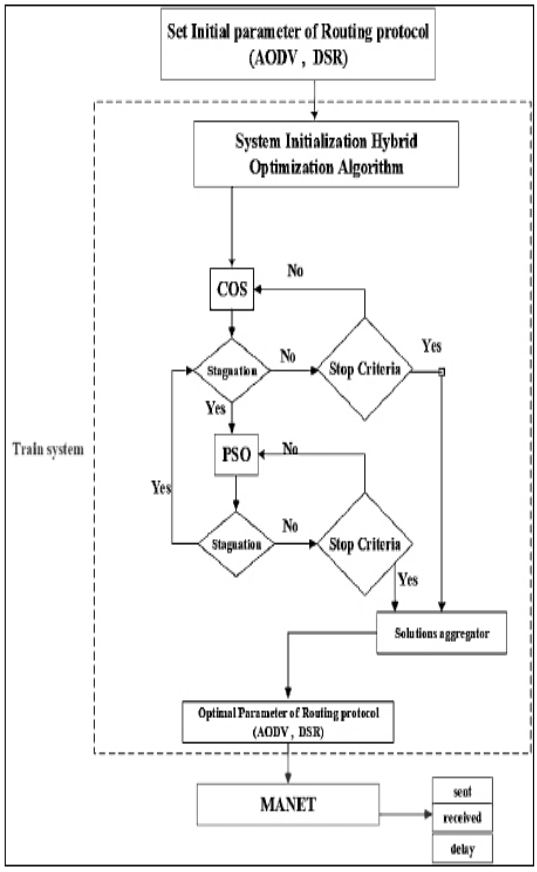

Figure 3 Proposed system

FINDING AND DISCUSSION

The proposed system would evaluate more than 10000 distinct scenarios using a variety of settings for the MANT routing protocol. The PSO and CSO algorithms, both of which are well-known in the field of metaheuristics, are contrasted with the suggested model. The default values for the general optimization parameters are as follows: the number of iterations is set to 10, the problem reduction is set to 3, and the population size is set to 20. The upper bounders of each particle are equal to 5, while the lower bounders are equal to -5. The primary parameter of the PSO algorithm is configured as follows: the constants values (c1,c2) are configured to have a value of (1.25), and the weight inertia is set to 0.5. The primary parameter of the CSO algorithm is configured as follows: the number of cats (NUM CATS) is set to 6, the percentage of seeking cat (MR) is set to 2, the seeking memory pool (SMP) is configured to 3, and the percentage - seeking range of the selected dimension (SDR) is configured to 10. The parameters for the hybrid model that was proposed (CPSO) were the same as those for PSO and CSO. In comparison to CSO and our own suggested model, the optimal outcome that could be satisfied by the PSO model was the poorest (CPSO). The optimal situation for PSO, in terms of the number of nodes (19), the number of connections (10), and the speed rate, is as follows: (10). A total of 162 packets were transmitted and received in the PSO's scenario (109). This is due to the delay in its situation (6023.5 Sec). In comparison to CPSO's findings, those obtained by CSO were not very impressive. The CSO determined that the optimal scenario consisted of 132 packets distributed among 19 nodes and 10 connections, and the average speed rate of each node was (10). The number of packets that are received by CSO is thirteen, and the delay time for this scenario is fifty-two and thirty-six seconds. The finest outcomes that our suggested system has achieved so far include fulfilling the optimal MANET scenario with (19) nodes, (4) connections, and the rate speed of mobile node as being 1. (4). CPSO identified the following object values: transmitted (48) packets, received (47) packets, and delay (6.13 sec). Table 2 presents a comparative analysis of PSO, CSO, and the proposed CPSO with regard to the number of dropped packets (DP), the percentage of successful packets (R/S), and the latency.

Table 1 Compere result over 30 runs of PSO, CSO, and CPSO

Algorithm	DP	R/S	Delay (sec)
PSO	53	0.346	6023.3
CSO	1	0.0076	52.36
CPSO	1	0.0076	6.13

Due to the power of the CSO in searching on the best possible solution in search space and this characteristic being inherited by the CPSO in order to increase the search progress, the CSO and the suggested CPSO have almost the same performance in terms of the number of packets that are dropped. The drop packets of over scenario that are selected by PSO, CSO, and CPSO are displayed in Figure 4.

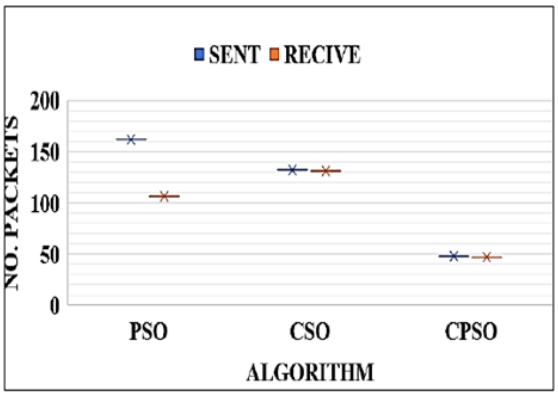

Figure 4 Compere drop packets of PSO, CSO and CPSO

CONCLUSION

The goal of this project is to design a fully protected, quality of service (QoS), and efficient routing-based optimization protocol for MANET by making use of the newest secured technologies, namely block chain and computational algorithms. Through pet and PDR, the optimization multi-objective seeks to locate the most effective route among the various possible combinations of delay and packet loss. Finding the best possible routing for many protocols, such as DSR, AODV, and DSDV, is the primary goal of this project. The findings will demonstrate that the optimised routing protocol is superior to the regular routing protocol.

REFERENCE

[1] Baisakhi Chatterjee (2019)" Parameter Training in MANET using Artificial Neural Network" I. J. Computer Network and Information Security, 9, 1-8

[2] Al-saeedi, A. H. (2016). Binary Mean-Variance Mapping Optimization Algorithm (BMVMO). *Journal of Applied and Physical Sciences*, *2*(2), 42–47. https://doi.org/10.20474/japs-2.2.3

[3] Boutaba et al. (2018) "A comprehensive survey on machine learning for networking: evolution, applications and research opportunities" Journal of Internet Services and Applications 9:16

[4] Bright SelormKodzoAnibrika (2020) "A Survey of Modern Ant Colony Optimization Algorithms for MANET: Routing Challenges, Perspectives and Paradigms" International Journal of Engineering Research & Technology (IJERT). ISSN: 2278-0181 Vol. 9 Issue 05

[5] D. E. Nayab et al. (2021) "Prediction of Scenarios for Routing in MANETs Based on Expanding Ring Search and Random Early Detection Parameters Using Machine Learning Techniques" IEEE. VOLUME 9,

[6] Dr. M. Duraipandian (2019) "Performance Evaluation of Routing Algorithm for Manet Based on The Machine Learning Techniques" Journal of trends in Computer Science and Smart technology (TCSST) Vol.01/No.01 Pages: 24-35.

[7] Habboush, A. (2019). Ant Colony Optimization (ACO) Based MANET Routing Protocols: A Comprehensive Review. *Computer and Information Science*, *12*(1), 82-92. https://doi.org/10.5539/cis.v12n1p82

[8] Kumar, S., Raghavan, V.S., & Deng, J. (2006). Medium access control protocols for ad hoc wireless networks: A survey. *Ad Hoc Networks*, *4*(3), 326–358. ttps://doi.org/10.1016/j.adhoc.2004.10.001

[9] Kumar, S.S., Manimegalai, P., & Karthik, S. (2018). An energy-competent routing protocol for MANETs: a particle swarm optimization approach. *In International Conference on Soft-computing and Network Security (ICSNS)*, 1-10.

[10] Mirjalili, S., & Lewis, A. (2013). S-shaped versus V-shaped transfer functions for binary particle swarm optimization. *Swarm and Evolutionary Computation*, *9*, 1-14.

[11] Sarao, P. (2018). Comparison of AODV, DSR, and DSDV routing protocols in a wireless network. *Journal of Communications*, *13*(4), 175–181.

[12] Yefa Mai, Yuxia Bai, & Nan Wang. (2017). Performance Comparison and Evaluation of the Routing Protocols for MANETs Using NS3. *Journal of Electrical Engineering*, *5*(4), 187–195. https://doi.org/10.17265/2328-2223/2017.04.003