RESEARCH ARTICLE

Performance Analysis of Cluster-Based Dynamic Multipath Trust Secure Routing (DMTSR)-Protocol in Wireless Sensor Networks (WSNs)

Darshan B D
Department of Electronics and Communication Engineering, SJB Institute of Technology, Bangalore, Karnataka, India.
darshan156@gmail.com

Prashanth C R
Department of Electronics and Telecommunication Engineering, Dr. Ambedkar Institute of Technology, Bangalore, Karnataka, India.
prashanthcr.ujjani@gmail.com

Received: 13 April 2023 / Revised: 01 June 2023 / Accepted: 07 June 2023 / Published: 30 June 2023

Abstract – A wireless sensor network [WSN] analyses the structured information supplied from the base station for the hostile environment. The primary drawback of WSN is Security since the sensors are placed in a closed network. WSNs are primarily disrupted by a variety of harmful 'internal and external' attacks. Due to these attacks, the leading resources in the networks, like power and memory, will be drained early. To overcome these problems, propose a novel protocol: Dynamic Multipath Trust Secure Routing Protocol (DMTSR) with Advanced AAODV protocol. For encryption and decryption purposes, Advanced Encryption Algorithms [AES] are used to help the above protocol. The fastest path is found to a destination from the source node by considering the neighbour node's energy level and energy consumption of the node. It can reduce packet loss and improve the packet_ delivery ratio. DMTSRP and AAODV protocols are merged to develop an innovative approach to routing the information. The DMTSR will give a layer-by-layer explanation. The source node's primary job is to identify the path by considering the neighbour node and approaches for the primary keys. Source nodes begin updating intermediate nodes in secured regions using an AES encryption algorithm. The DMTSR protocol replaces packets of data. The DMTSR protocol uses a secondary_key to substitute an intermediate node, where the secured data is received at the final nodes. The simulation outcomes of the DMTSR protocol achieve a 92% Packet_Delivery_Rate, Throughput of 97%, and a delay is 0.278ms in the network.

Index Terms – WSN, AAODV, DMTSR, AES, Security, Cluster Head (CH), Routing Protocols, QoS.

1. INTRODUCTION

The WSN is the virtual network used for communication. The WSN does a lot of development and research. The primary method of communication for the nodes in the WSN is without the need for physical media. Each node's primary method of communication is via signals [1]. Sending packets to each node that will transmit signals is the WSN's job. Environmental monitoring, acoustic sensing, earthquake detection, target tracking, inventory tracking, health monitoring, and bright space are the main applications of WSNs [2].

WSN encounters a great deal of difficulty with attacks and gets a great deal of offense from the users. The effect, data integrity, power use, routing, and other characteristics of these attacks are categorised. Integrity and safety are major issues, even though the user has additional choices to do. It is easier for other users to attack the unguided transmission medium. Compared to the directed transmission medium, it causes challenges for the user. Instead of using an unstable medium, secure data transmission is prioritized [3-4].

The essential components of WSN security are Security & key management, authentication, Energy efficiency, secure routing, and resistance against node capture. The security and privacy of the most recent cryptographic methods exhibited less progress [5]. Latest studies have flashed that for the integrity & security of the WSN, the DMTSR protocol with Advanced AODV protocol is employed. The conventional AODV routing is replaced by the Advanced AODV routing. The data integrity and extended life lifetime of the WSN are both improved by the advanced AODV routing. The maximum energy for battery life and sensor node probability is used in advanced AODV routing. In recent research, a wireless sensor network with an advanced AODV mechanism, which is powered by an external battery that is located outside—was the subject of attention. The new method uses advanced routing to determine the best path for maximizing energy use. The nodes in varied activities, transmit, and appropriate sleep modes lost energy. The minuscule routing uses several energy nodes to go from source to destination. Advanced AODV routing saves energy by locating the nodes that are close to the sensor nodes [6-7]. In this case, the route forwarding technique provided the exact route. The path of this algorithm is used to test.

The point of the study is to demonstrate how to utilize DMTSR protocol in conjunction with a Data encryption approach to avoid the distribution of source routes. The DMTSR protocol employs a technique known as layer-by-layer decryption. The most straightforward approach to identifying a node is to gather the primary keys for the relay node. Packets of data that utilize the DMTSR protocol route with the secondary key for each intermediate node. Data is protected from Intruders through AODV, DMTSR, and AES encryption. Secure data forwarding nodes ensure that the network's data transmission is reliable.

The research was broken up into several pieces. The review of the available literature is one area of interest. Secured quality of service in wireless sensor networks is the subject of this literature review. The incorporation into the standard procedure known as the DMTSR protocol is the subject of another section. The results and conclusions from the examination of the simulators are rendered in the deciding section.

WSNs utilize a variety of energy-efficient routing strategies to improve performance. Each approach says its drawbacks, and the intended application determines the best architecture to use. Figure 1 displays a few such methods. The main difficulty for WSN is to find a method that uses the least amount of energy while yet delivering accurate sensor information to the sink node. The computational complexity of data_collection, data_aggregation, and data_delivery, as the total energy consumption of the node, have been reduced using several techniques.

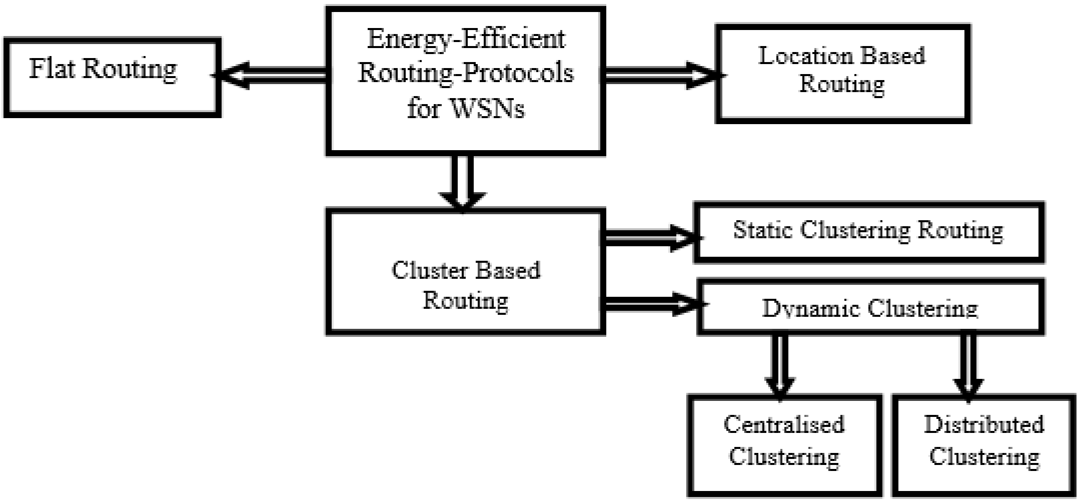


Figure 1 WSN Routing Protocol Classification

The amount of time spent in communication between nodes is directly proportional to the reliability of WSNs. Because of the constraints imposed by sensor nodes' architecture and communication protocols, this can only be accomplished by making effective use of the available energy. Communication congestion occurs as a direct consequence of a rise in both the complete nodes and WSN's overall area. The packet delivery ratio of communication is impacted because of the congestion, which may lead to a decrease in their performance. As a result, optimal performance requires careful attention to both the routing of vehicles and the control of traffic congestion [8]. In the past, a few different ideas for energy-efficient data routing protocols were offered. These kinds of algorithms are split up into different classes: (i) flat_routing, (ii) location-based, and (iii) hierarchical_routing. Additional expansions using spatial routing algorithms have also been suggested as a means of enhancing the reliability of the network. In WSNs, the hierarchical clustering approach is superior to both the centralized and the flat routing approaches in terms of efficiency.

In this method, several clusters make up the whole network. From the respective cluster, choose a node to serve as cluster head (CH) using statistical and probabilistic methods. A node has a better probability of getting picked as a cluster head if it has higher residual energy. These CHs oversee gathering information from each of their clusters and sending the aggregated information to the BS. The authors were constantly inspired to conduct studies using new computational parameters by certain clustering strategies, including cluster creation, CH selection, and cluster size. Static clustering involves a single cluster creation that lasts until the end of the whole network. The majority of the techniques concentrate on lively clustering. In this, clusters are continually constructed through the course of a WSN depending on the condition of the node density, residual_energy, and further variables. The main functions of each sensor node are memory management, internal computation, environment sensing, and code execution.

Many node states may exist in WSNs after cluster creation. A node can be one of the following: (1) an Autonomous Node; (2) cluster_head applicant; (3) Head of a cluster; (4) Cluster_member (5) Assistant head of a cluster; (6) a momentary node assists as an association between the cluster-head and cluster-members. The nodes in various states are tasked with additional duties. The essential duties of each kind of sensor node Cluster-head different nodes are shown in Figure 2. The total energy at the sensor nodes is quickly depleted because of these extra duties. The location of nodes and sinks is the most difficult task in the creation of WSNs. Meanwhile, the communication range of these tiny devices is very limited [9-10].

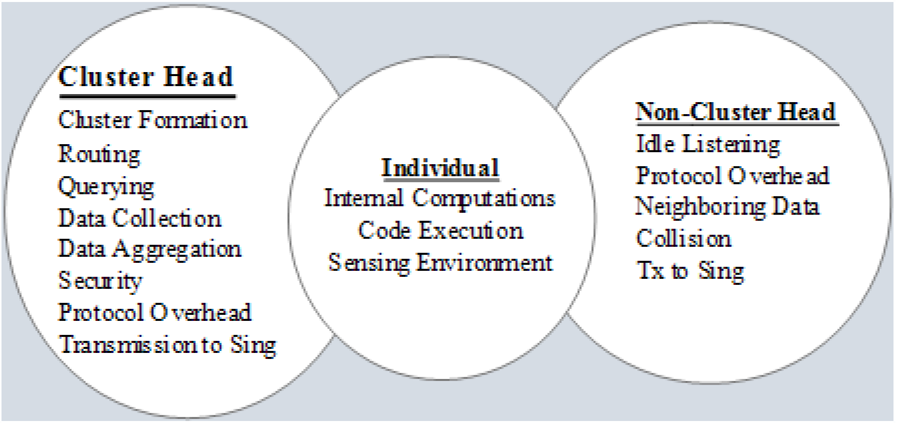


Figure 2 Common Energy-Consuming Tasks

As indicated in Figure 2, the transmission phase is when a node expends most of its energy. A CH will use more energy during the transmission phase if it is further from the base station (BS) or sink than CHs that are closer to the BS. To control coverage in bigger regions and network stability, several previously-standing routing approaches are expanded for multi-hop strategies [11-12]. It was found that adding nodes with more energy resulted in improved performance. More stability is provided by the nodes' heterogeneity in terms of residual energy. The next section discusses a few methods, including heterogeneous nodes. To limit the amount of data sent at CHs, several researchers concentrated on sophisticated data aggregation methods, which often overloaded the CH nodes and lengthened transmission delays.

The organizations of the paper are Section-1 detailed introduction to the Wireless Sensor Network. Section-2 details the literature review. In Section 3, the detailed proposed work, along with the procedure, is discussed. The experimental outcome is elaborated on in Section-4, and the Conclusion is discussed in Section 5.

2. LITERATURE SURVEY

K. Maheshwar et.al., [1] came up with a new way to group things. They called it bioinspired WSN clustering. Clustering techniques are often employed to reduce energy, but they may also be utilized to achieve other efficiency goals and propose an improved ant colony optimization algorithm.

Mittal et.al., [2] presented Moth-Flame-Optimization (MFO), and Threshold-sensitive-Energy-Efficient Clustering Protocol (TECP) for increasing its stability. Clustering the network with the usage of congestion control is an NP-hard problem; thus, a preeminent technique was used to accomplish it. It provides an analysis of the simulation study that proved that the suggested technique may perform better than alternative protocols. It motivates us to propose a new model considering the control overhead, system lifespan, and energy consumption.

Ahmad et.al., [3] came up with a novel method to choose the CH dependent on the ABC optimization, and they suggested it. The optimization algorithm was calculated by the amount of remaining energy, the base station distance, and the distance between clusters. Cluster heads are chosen by applying an optimal fitness function to each cluster's selection process, and the work being suggested will cut down on the aggregate of energy used. Considering this approach, propose a new method of Cluster head selection model that performs fine than other standard techniques.

Jiang et.al., [4] come up with Parallel-CSS (PCSS) protocol to preserve power in WSN. The presentation covered two distinct communication tactics, each of which was applied to a different set of circumstances. In comparison to PSO and CSS, the suggested PCSS has a higher level of convergence. If an incorrect option is done on Cluster-head, it may result in greater power utilization, which would reduce efficiency.

Lee J et.al., [5] proposed an enhanced version of the 3-Layer Low-Energy-Adaptive-Clustering Hierarchy for WSNs. These authors created it to enhance the energy efficiency of the network and to extend its lifespan. The decrease in energy feeding and the extension of the lifetime of WSNs are the primary focuses of this article. The performance level is inadequate, which is another disadvantage of this research, which also introduces the LEACH protocol. The outcome of the simulation demonstrates superior performance in comparison to that of others.

Shariq et. al., [6] proposed a new protocol, the Robust Cluster Based Routing Protocol (RCBRP), to find the best-optimized path. The plan is broken down into different stages so that we can investigate the communication. The author suggested a pair of algorithms, such as (1) an algorithm for cluster and route. (2) Computation method. The strategy reduces the volume of energy used and distributes the load more evenly by clustering the intelligent devices. The results of this study show that the suggested scheme is superior to its equivalents in terms of the sum of energy it consumes.

Vidhya et. al., [7] proposed a new multi-layer-security-protocol (MLSP) with EPC AODV protocol. The AES protocol uses the above-mentioned protocol to code & decode using the most important two techniques. In EPC-AODV, the aim is to discover the S-path possible by using the energy usage of the Neighbor node. WSN will be received in this manner with a minimal amount of packet loss. A technique to alter and be cautious for MLSP using EPC-AODV was created, and it was intended as a source path. The MLSP is going to oversee the layer-by-layer interpretation.

Younis et al. [8] came up with a hierarchical clustering-task scheduling policy (HCSP) that uses node-driven clustering instead of time-driven clustering like GRBP. According to HCSP, each cluster will only undergo a configuration change once throughout the course of each local super round. As an outcome, the rate of cluster reconfiguration shifts based on the request, and it's possible that it'll be different from one cluster to the next over the lifespan of the network. On the other hand, towards the conclusion of every global hypercycle, global clustering is carried out to revise the whole of the network structure. Therefore, the goal of HCSP is to produce a clustering-task scheduling that is more adaptable, efficient with energy use, and scalable than that of GRBP. Nabrdalik et al. [9] have come up with a plan to build and implement in testing ground networks an aware routing protocol known as SLE-AODV to ensure secure communication in a broad area WSN. A combination of AODV & LEACH was used in the creation of SLE-AODV (LEACH). It encrypts the data that is being transferred using AES (Advanced Encryption Standard) (AES). Experiments that were carried out in the lab produced data that confirmed considerable energy savings, which in turn led to an improvement in network lifespan.

Poulkov et al. [10] have come up with a protocol that they call the "Adaptive Sectoring Scheme for Reliability." This Procedure is applied to the transport of data that is trustworthy while also being energy efficient. In this technique, a particular sensor ground is partitioned into subfields that are conveyed into action one at a time when a certain event takes place. The sectoring process is constantly modified in accordance with a predetermined dependability of the data transmission to optimize the packet delivery ratio, limit the amount of congestion that occurs, and enhance the amount of energy that can be protected. The outcomes of simulation studies reveal that the projected approach results in an improvement in both the dependability and the amount of energy used.

3. PROPOSED WORK

3.1. System Architecture

WSNs find their most momentous applications in the fields of national defense, military applications, and healthcare. In contrast to further sensors, which have partial power, storage, and execution capabilities, the protection system must constantly be energy efficient and have a substantial quantity of storage capacity. The objective of this exploration is to use the NS2 network simulator to recreate a cryptographically secure network and set of data.

Figure 3 is an architectural diagram representation of the proposed work. Better results with safe data transmission utilizing QoS settings and PDR are accomplished by employing the DMTSR protocol with AES with AML encryption.

3.2. System Security

When the network interacts with the surroundings of its owner, security becomes an increasingly critical component of the system. In the absence of any form of security, performing network analysis without the involvement of human beings is an extremely challenging undertaking. The spirit of the resources, along with the truth that the protocol for security must be created, makes this a difficult task. The method that is utilized for the purpose of security is the transition from fixed to wireless networks [13-17].

3.3. Nodes Deployment

The sensor nodes observed the whole environment, both in and around it, and sent the data they collected onto the sink.

The data were acquired by the sensor nodes. The usual sensor nodes are the primary topic of attention in the current investigation. The origin node is responsible for sending data-packets at a point in the network when the information is being transferred from the sink to the other sink. A unique identifier (ID), main key, and secondary key will be generated for each node that has registered with the server. The objective of the node is to locate the most capable route that is developed in the main key being organized for all the middle nodes. The main (primary & secondary) keys will be present in every node. To ensure everyone's safety, and responsibility of the system is to monitor the communication going on among the nodes.

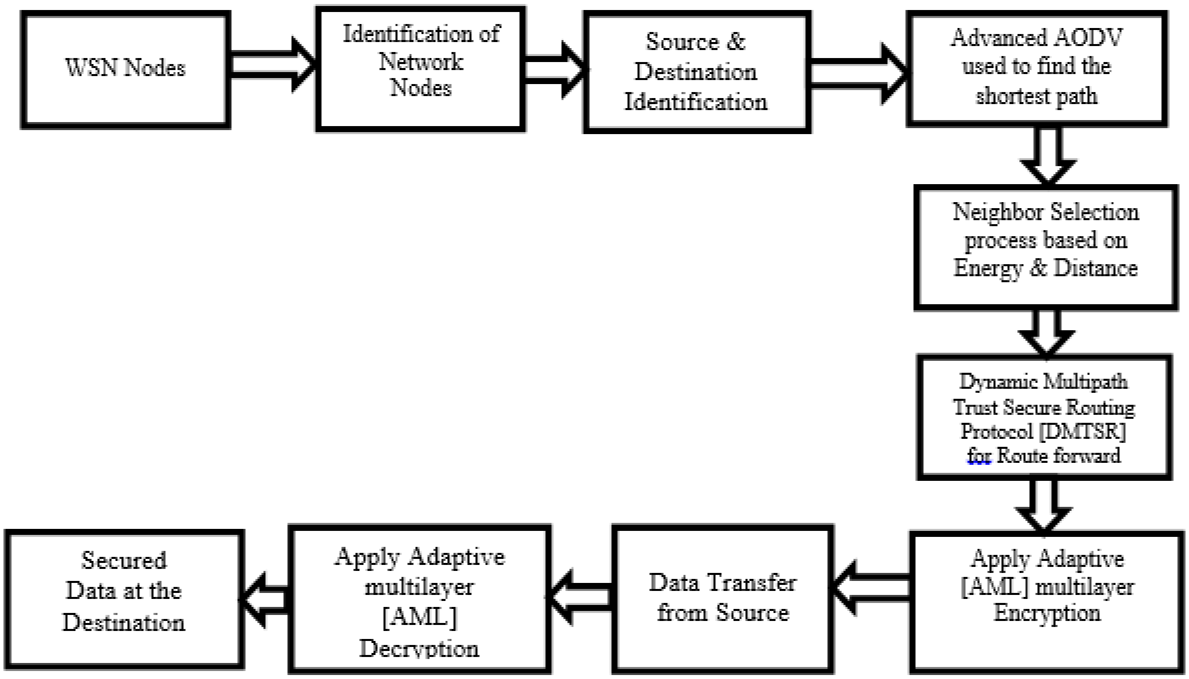

WSN Nodes
Identification of Network Nodes
Source & Destination Identification
Advanced AODV used to find the shortest path
Neighbor Selection process based on Energy & Distance
Dynamic Multipath Trust Secure Routing Protocol [DMTSR] for Route forward
Apply Adaptive [AML] multilayer Encryption
Data Transfer from Source
Apply Adaptive multilayer [AML] Decryption
Secured Data at the Destination

Figure 3 Architecture of Proposed System

3.4. Advanced-AODV (AAODV) for Shortest Route

The suggested work will look at the functioning of WSNs using an AAODV mechanism with an exterior battery power source. The position in a setup where the most energy is available may be found to have the best forwarding using Advanced AODV as well as the energy consumption technique [12]. All nodes demand an equal amount of external energy while routing data. The total power consumption technique is the managing strategy used to procure external energy sources. The approach accounts for energy depletion at the distinct nodes, regardless of whether they are active, sleep, transmit, or receive. This is because energy depletion happens concurrently at all nodes. Through routing, the neighbour who has the greatest amount of accessible power for transmission is selected. Choosing a neighbour becomes an easy and straightforward procedure when done in this manner [18-20]. Furthermore, the energy that would presently exist in the system is preserved in its current condition.

3.5. Dynamic Multipath Trust Secure Routing Protocol – DMTSR

Both the AES encryption approach and the DMTSR protocol are applied in the procedure of securing and guaranteeing the privacy of routes. The DMTSR protocol offers a decryption method that works from the bottom up, layer by layer. The sources that gather the main key for each intermediate node are the ones that will be able to find the best route. Each node has a main key as well as a secondary key associated with it. Using a multilayer routing procedure that has security enabled, information may be sent across WSNs and converged at a central location [21]. Many distinct forwarding protocols for WSN have been suggested by academics both in the United States and in other countries. In this part, a good many of the standard security procedures are broken out in detail. From the use of multilayer routing, it is possible to obtain a large development in the rate of successful submission of data packets. It is also proficient in balancing the amount of energy a node consumes, which in turn allows for the node's lifespan to be extended, as shown in Algorithm 1.

Adaptive Multi-Layer routing is a good way to keep selective forwarding attacks from happening. This protocol considers the problem of duplicate data, and the nodes are linked together so that the information can be combined. This makes it easier to send data and saves network energy at the same time [22-25].

```
Begin (); {
Initialize nodes (50);
Initialize source and designation nodes;
Initialize nodes and set keys (k1,k2);
for i = 0 – n
do {
Vni Mx( E);
Vni = MLSP( );
Sa; Attribute of Sensor
Hv Hard value(i);
Sv Soft value(j);
P Packet of Data;
Ri Energy;
Fg Flag;
if Sa ≤ Hv & Ri> 0, Tn
send_P
set_Fg = 1
else-if Sv ≤ S < Hv AND Ri > 0 Tn
send_P
set Fg = 0
else
transmission=No
end if
if (N = Rng (Vni)) Tn {
Node forward (Transmitted);
Ni to Sp (node);
else
N is under Lni
end if
end }}
for i = 0 – n
do {
for j = j+1 - n do {
Vnij nodes collect key(k1)
if (Nk = = Ik) Tn {
N = Ep (key)
send Key;
If (K = Sk) {
end if }
Sn forward Ed(P);
if (Vni) Tn {
Fd Dn
else
Fd Lnij
Vni Dn
end if
Dn Decry(P);}}}
End
```

Algorithm 1 DMTSR

3.6. Adaptive Multilayer Encryption Process

Encryption is the technique of compelling information incomprehensible without specialized knowledge. This process is known as the procedure of providing knowledge unbreakable. Encryption has been used to provide communication security for centuries, and now, the only people and organizations that make use of this technology are those that have very stringent security requirements [16]. Even though encryption may make information safer, there is still a need for other types of communication protocols to ensure comprehensive security. This is because encryption alone is not enough. Other methods, such as message authentication codes (MAC) are required to establish whether or not a given message has been tampered with and whether or not its integrity has been maintained [26-28].

Cryptography is the study of coding and decoding data using mathematics as the underlying mathematical theory. The AES encoding method is started as soon as the source node determines the smallest route by gathering all of the intermediary nodes' main keys. Figure 4 depicts the AES algorithm's encryption procedure. Using the secondary key to the intermediary nodes, data packets were decoded using the

DMTS routing mechanism. The secure information of Nodes data, with the Node-ID and connected data, are obtained in this manner by the destination nodes [29]. The source chooses the best route, which gathers the main key from all intermediary nodes. Each node has a secondary key and a main key that match.

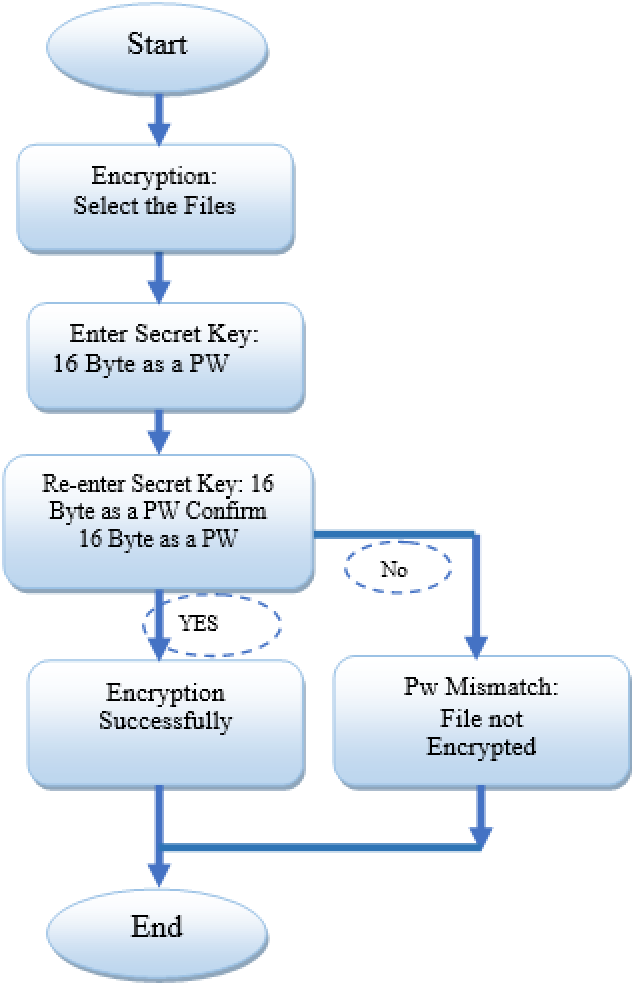


Figure 4 Encryption Process

3.7. Decryption Process

The user is necessary to provide the alike Secret Key that was provided during the process of encrypting the file before the decryption process can begin. This occurs after the process of encrypting the file is complete. If the Secret Key that was used throughout an encryption process is the same one that was used to decrypt the file, then it will be able to successfully decrypt the file. If this condition is not met, an error message will be shown. By using the same encryption key and doing the transformation in the other direction, it is possible to convert cipher text back into the original plain text. This is done by using a sequence of reverse rounds.

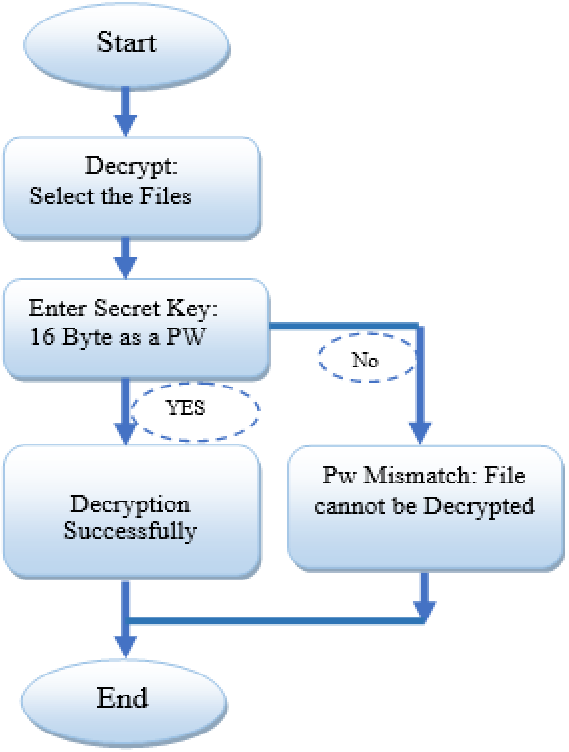


Figure 5 Decryption Process

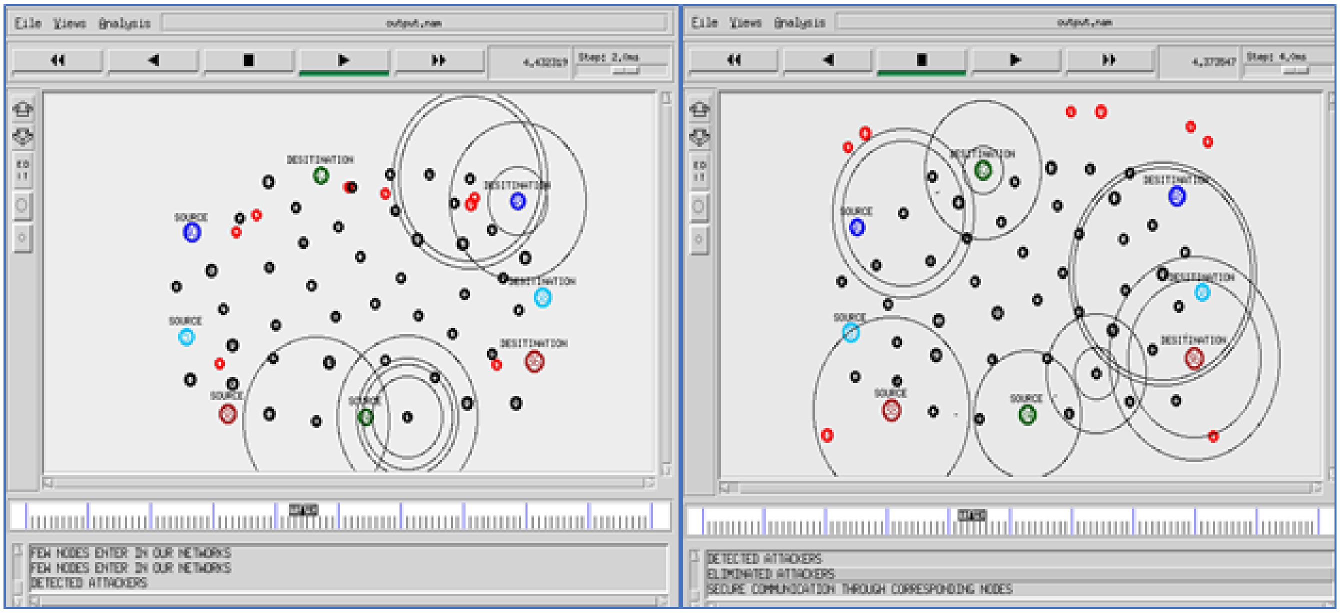
The data is then sent to a target node when the neighbour node has encrypted the packet it contains. The process of decryption using the AES algorithm is shown in Figure 5. It is possible to identify the presence of a new node in a network even when none of the other nodes in the network are specified [30]. The destination node makes use of the AES technique to decrypt the packet with the assistance of the S-key. In the last step, the data in its original form is examined by the receiver node. If there is a dynamic fluctuation associated with the ability of the pathways, paths vary in real time according to the information transfer activity that is taking place across a network [20]. Therefore, the PDR improves, and the average time from start to finish falls.

3.8. Working Procedure of Encryption and Decryption Process

1. The encryption process is initiated by selecting the file.
2. The secret_key is implemented as 16-byte passwords.
3. Re-entering the 16-byte password for confirmation. And then select Encryption.
4. The converted file is stored in the disc.
5. The converted file is decrypted by selecting the decryption.
6. The encoded file is secured, and this file is protected from the delete option.

4. RESULTS AND DISCUSSIONS

The Network-Simulator-2 (NS-2) is used to simulate the proposed scheme by considering the parameters under the performance index incorporated with the DMTSR proposed scheme. Some Parameters are listed in Table 1 that supports the Simulation.



```
FEW NODES ENTER IN OUR NETWORKS
FEW NODES ENTER IN OUR NETWORKS
DETECTED ATTACKERS
```

```
DETECTED ATTACKERS
ELIMINATED ATTACKERS
SECURE COMMUNICATION THROUGH CORRESPONDING NODES
```

Figure 6 Scenario of Detection of Attacker Node

Simulated results exhibit that the suggested technique works well when several factors are considered. It shows how the separate methods are compared in the literature. Both AODV and MLSP were used, both of which were used as technical baselines. The attacker node detection scenario is shown in Figure 6.

Table 1 Simulation Specifications

Specifications	Quantity
Simulator	NS-2
Number of nodes	50
Range of Transmission	250m
Size of Packet	1000 bits
Range-Tx	100 KB
Antenna Type	Omni-Directional
RF	850–950 MHz
Routing_Protocol	Advanced AODV
MAC_protocol	IEEE 802.11
Packet-Interval	0.01 s

4.1. Energy/Power Consumption

It is the total amount of power used for broadcast and handling of data. Figure 7 illustrates variations in the network's energy usage for nodes ranging from 50 to 1000. The network's energy use ranges to its maximum value of 14.0 J when 50 nodes exist in the network. The rate of energy usage decreases as the number of nodes is raised from 50 to 250. A gradual reduction in the extreme energy usage of the system is shown when the nodes are raised from 250 to 750.

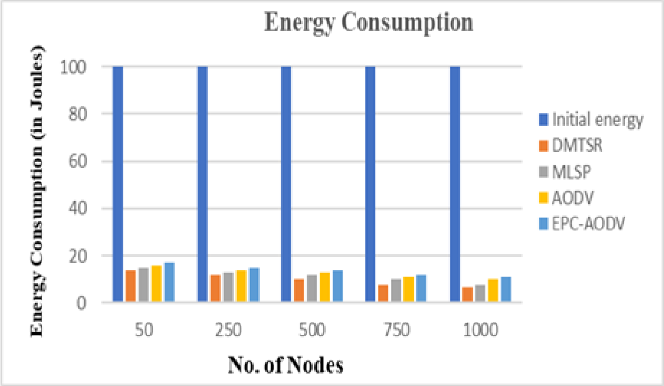


Figure 7 Energy Consumption

If the 750 nodes are present in the network, it consumes more energy that is 8J. When the 1000 nodes are present in the network, which is observed to lower values of energy usage is 7 J.

Its minimum value is relative. The typical energy usage in comparison to different approaches, such as AODV, MLSP, and EPC-AODV methods. Compared to the existing approaches, the DMTSR provides better results.

4.2. Packet-Delivery-Ratio

The packet delivery ratio measures how many data packets a node can send in a given amount of time. If you want to see how well the Energy characteristics and duplication reduction are working, compare the PDR to a standard WSN.

Figure 8 provides a graphical representation of this comparison. For a network per 50 nodes, the suggested detection system achieves a 92%. If the network with 250 nodes, this figure drops to 90%. If the network with few nodes, the PDR increases rapidly. The curve again increases to a point when the PDR is 89% for 500 nodes in the network. The maximum value of the curve is 84% for 750 nodes in the network. However, this value drops to 83% when the number of nodes in the network is raised from 750 to 1000. Overall, packet delivery is greater than the approach's 83% estimate, as shown in Table 2. There is a correlation between the packets sent and the ones received, and this correlation is measured by the PDR. If the packet delivery ratio is high, the protocol is functioning well. Various approaches, such as AODV, EPC-AODV, and MLSP, are evaluated concerning the PDR. When associated with conventional methods, DMTSR's recommended solution produces superior results.

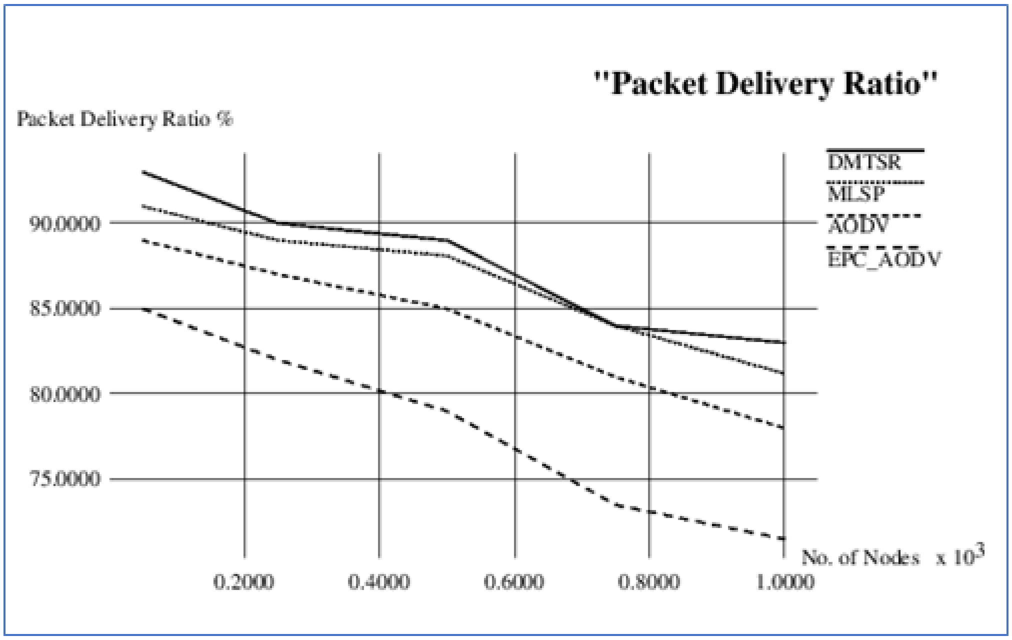


Figure 8 Packet-Delivery-Ratio Performance

Parameter	Packet Delivery Ratio				
Nodes	50	250	500	750	1000
DMTSR Proposed	92	90	89	84	83
MLSP	91	89	88.1	84	81.2
AODV	89	87	85	81	78
EPC-AODV	85	85	79	73.5	71.5

Table 2 Comparison of PDR

4.3. End-to-End Delay

End-to-End latency is the time required for each node to receive the packet and retransmit it. The comparison's outcome shows that there is less latency in the proposed model compared to the existing approaches in WSN, as shown in Figure 9.

If the network with 50 nodes, the delay is measured at a minimum of 0.115ms. The end-to-end latency for 250 nodes is 0.178ms. The end-to-end latency for 500 nodes is 0.195 ms. The arc achieves a value of 0.201ms for the network's end-to-end delay for 750 nodes. The curve for end-to-end network delays goes to a value of 0.278ms for 1000 nodes in the system. The delay shows that when a network has the fewest nodes, the delay is minimum, and the nodes are more. There is a slight increase in the delay shown in Table 3. The amount of time it takes an average data packet to reach its destination is known as the average end-to-end latency.

Table 3 Comparison of End-to-End Delay

Parameter	End-to-End Delay				
Nodes	50	250	500	750	1000
DMTSR Proposed	0.115	0.178	0.195	0.201	0.278
MLSP	0.123	0.182	0.198	0.206	0.284
AODV	0.182	0.24	0.31	0.395	0.58
EPC-AODV	0.261	0.45	0.69	0.786	0.99

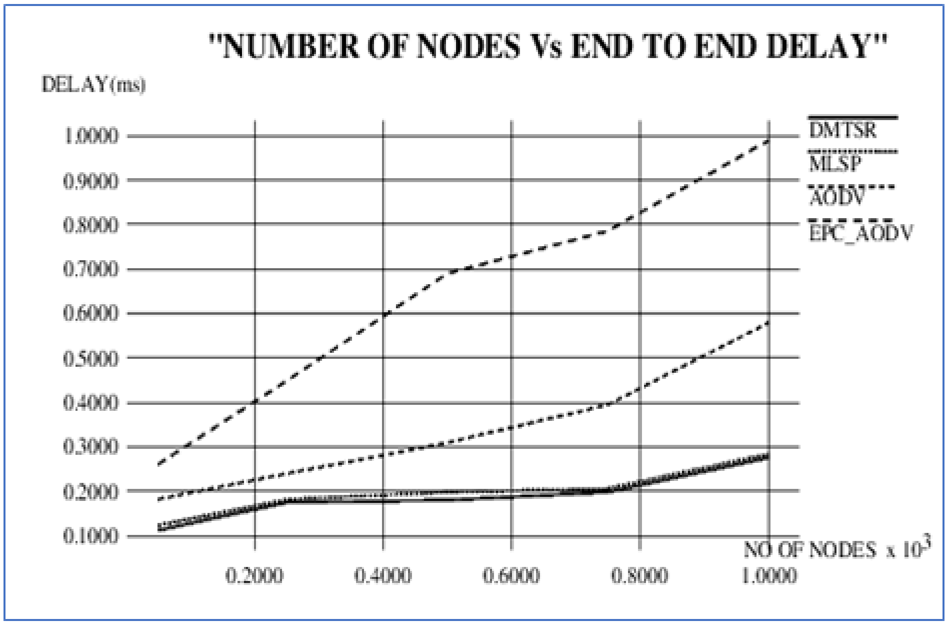


Figure 9 End-to-End Delay Performance

A protocol's end-to-end delay and performance are inversely related, the end-to-end delay assessment in comparison to AODV, MLSP, and EPC-AODV, among other methodologies. When related to other techniques, the suggested method, DMTSR, yields better results.

4.4. Throughput

The amount of packet transfers that a particular node can typically handle is referred to as its "throughput." The results of this throughput comparison between a conventional WSN and an improved WSN show that the latter outperforms the former.

The comparison of the throughput for a different set of nodes is shown in Figure 10. Based on the throughput curve, it appears that a performance enhancement of 97.5% has been attained. When the 50 nodes are in the network, the throughput value reaches 66%. When there are 250 nodes in the network, the throughput curve reaches 70% of its potential. If the 500 nodes are present in the network, the throughput goes up to 81%, which is a significant gain. When the number of nodes in the network is 750, there is a corresponding rise in the amount of data that can be sent to 89%. This demonstrates that the work that was recommended will be carried out effectively. When the network node size is increased to 1000, the throughput curve shows 89.5%, bringing the total to 97.5%. Comparisons of throughput performance are shown in Table 4, and the methodologies and methods included include AODV, MLSP, and EPC-AODV, among others.

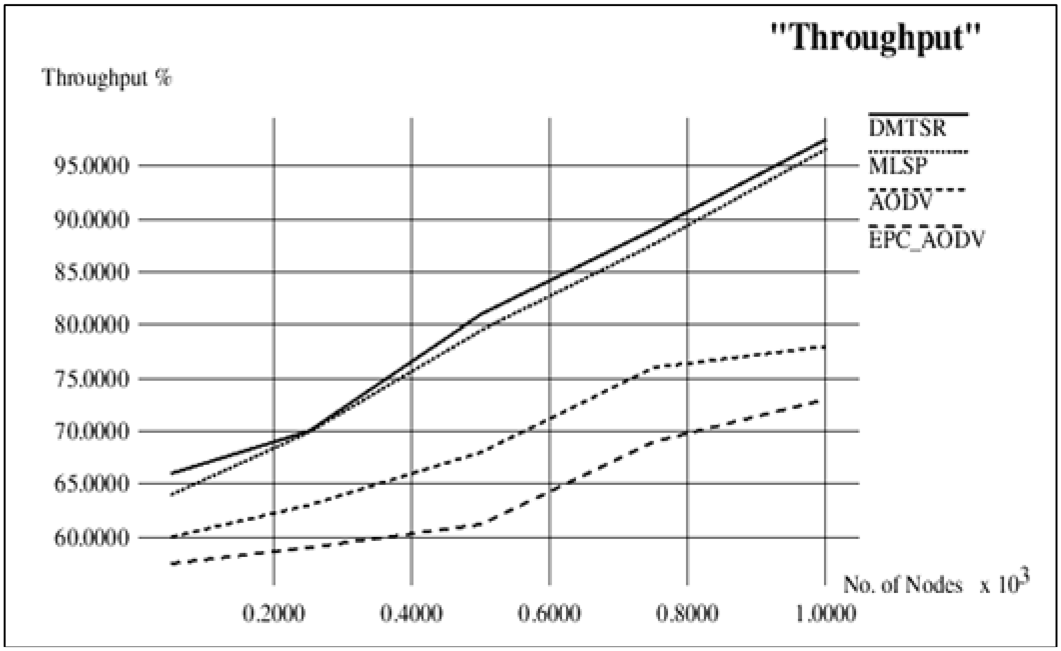


Figure 10 Throughput Performance

Table 4 Comparison of Throughput

Parameter	Throughput				
Nodes	50	250	500	750	1000
DMTSR Proposed	66	70	81	89	97.5
MLSP	64	69.9	79.5	87.6	96.6
AODV	60	63	68	76	78
EPC-AODV	57.5	59	61.2	69	73

5. CONCLUSION

To execute the DMTSR, the Network Simulator-2 is used (NS2). By dynamically adjusting broadcast power and routing choices, WSN ensures safe transmission at the lowest possible energy cost while still meeting the communication latency needed by applications. The author’s approach is meant to focus on the QoS & security of sensor networks and energy Consumption. Compared to other routing protocols, this one is more reliable because it reduces the number of dropped packets and the time it takes to get from one end to the other. The AMLSP technique, which uses energy-aware routing, is effective in the position of both protection and energy use. In the future, the effort can be made bigger by adding different kinds of attacks and security measures. This method is used in military applications to find intruders with better security mechanisms.

REFERENCES

[1] K. Maheshwar, S. Veenadhari, and S. Almelu, “Performance analysis of energy efficient optimization algorithms for cluster-based routing protocol for heterogeneous WSN,” Lecture Notes in Electrical Engineering, pp. 631–643, 2022.

[2] Mittal, N. (2019). Moth flame optimization-based energy efficient stable clustered routing approach for wireless sensor networks. Wireless Personal Communications, 104(2), 677–694.

[3] Ahmad, T., Haque, M., & Khan, A. M. (2019). An energy-efficient cluster head selection using artificial bee’s colony optimization for wireless sensor networks. Advances in Nature-Inspired Computing and Applications (pp. 189–203). Cham: Springer.

[4] Jiang, T. B., Chu, S. C., & Pan, J. S. (2020, October). Parallel charged system search algorithm for energy management in wireless sensor network. In 2020 2nd International Conference on Industrial Artificial Intelligence (IAI) (pp. 1–6). IEEE.

[5] Lee, J. and Kao, T. An Improved Three-Layer Low-Energy Adaptive Clustering Hierarchy for Wireless Sensor Networks. IEEE Internet of Things Journal, 3(6), pp.951-958, (2016).

[6] M. Shafiq, H. Ashraf, A. Ullah, M. Masud, M. Azeem, N. Z. Jhanjhi, and M. Humayun, “Robust cluster-based routing protocol for IOT-assisted smart devices in WSN,” Computers, Materials & Continua, vol. 67, no. 3, pp. 3505–3521, 2021.

[7] S. Vidhya and T. Sasilatha, “Secure data transfer using Multi-Layer Security Protocol with energy power consumption AODV in wireless sensor networks,” Wireless Personal Communications, vol. 103, no. 4, pp. 3055–3077, 2018.

[8] Neamatollahi, P., Abrishami, S., Naghibzadeh, M., Yaghmaee Moghaddam, M. and Younis, O. Hierarchical Clustering-Task

Scheduling Policy in Cluster-Based Wireless Sensor Networks. IEEE Transactions on Industrial Informatics, 14(5), pp.1876-1886, (2018)

[9] E. Niewiadomska-Szynkiewicz and F. Nabrdalik, "Secure low energy AODV protocol for Wireless Sensor Networks," 2017 27th International Telecommunication Networks and Applications Conference (ITNAC), 2017.

[10] M. Chaudhari, P. Koleva, V. Poulkov, and O. Asenov, "Multilayered distributed routing for power efficient Manet Performance," Wireless Personal Communications, vol. 97, no. 2, pp. 1729–1752, 2017.

[11] S. Alkhliwi, "Energy efficient cluster-based routing protocol with secure ids for IOT assisted heterogeneous WSN," International Journal of Advanced Computer Science and Applications, vol. 11, no. 11, 2020.

[12] S. Padaganur, P. S. Patil, and M. Deshmukh, "Performance analysis of Cluster-based energy-efficient routing scheme for WSN," Soft Computing for Intelligent Systems, pp. 417–424, 2021.

[13] Z. Wang, H. Ding, B. Li, L. Bao, Z. Yang, and Q. Liu, "Energy efficient cluster-based routing protocol for WSN using Firefly algorithm and ant colony optimization," Wireless Personal Communications, vol. 125, no. 3, pp. 2167–2200, 2022.

[14] P. Nandhini and A. Suresh, "Energy efficient cluster-based routing protocol using charged system harmony search algorithm in WSN," Wireless Personal Communications, vol. 121, no. 3, pp. 1457–1470, 2021.

[15] S. Akila and R. Venkatesan, "An energy balanced geo-cluster headset based multi-hop routing for wireless sensor networks," Cluster Computing, vol. 22, no. S4, pp. 9865–9874, 2018.

[16] M. Bilal, E. U. Munir, and F. K. Alarfaj, "Hybrid clustering and routing algorithm with threshold-based data collection for heterogeneous wireless sensor networks," Sensors, vol. 22, no. 15, p. 5471, 2022.

[17] R. Rajeswari, K. Kulothungan, S. Ganapathy, and A. Kannan, "Trusted energy aware cluster-based routing using fuzzy logic for WSN in IOT," Journal of Intelligent & Fuzzy Systems, vol. 40, no. 5, pp. 9197–9211, 2021.

[18] H. Yetgin, K. T. Cheung, M. El-Hajjar, and L. Hanzo, "A survey of network lifetime maximization techniques in wireless sensor networks," IEEE Communications Surveys & Tutorials, vol. 19, no. 2, pp. 828–854, 2017.

[19] M. Shafiq, H. Ashraf, A. Ullah, M. Masud, M. Azeem, N. Z. Jhanjhi, and M. Humayun, "Robust cluster-based routing protocol for IOT-assisted smart devices in WSN," Computers, Materials & Continua, vol. 67, no. 3, pp. 3505–3521, 2021.

[20] B. Han, F. Ran, J. Li, L. Yan, H. Shen, and A. Li, "A Novel Adaptive Cluster Based Routing Protocol for energy-harvesting wireless sensor networks," Sensors, vol. 22, no. 4, p. 1564, 2022.

[21] S. Chelbi and R. Moussi, "A cluster-based routing protocol and Fault Detection for Wireless Sensor Network," International journal of Computer Networks & Communications, vol. 13, no. 04, pp. 71–83, 2021.

[22] L. M and P. C R, "Designing an energy efficient clustering in heterogeneous wireless sensor network," International journal of Computer Networks & Communications, vol. 13, no. 1, pp. 75–92, 2021.

[23] Y. El Assari, S. Al Fallah, J. El Aasri, M. Arioua, and A. El Oualkadi, "Energy-efficient multi-hop routing with unequal clustering approach for wireless sensor networks," International journal of Computer Networks & Communications, vol. 12, no. 3, pp. 55–73, 2020.

[24] M. Rajasekaran, "Performance and evaluation of Location Energy Aware Trusted Distance Source Routing Protocol for secure routing in wsns," Indian Journal of Science and Technology, vol. 13, no. 39, pp. 4092–4108, 2020.

[25] S. Smiri, A. Boushaba, R. Ben Abbou, and A. Zahi, "Performance analysis of routing protocols with roadside unit infrastructure in a vehicular ad hoc network," International journal of Computer Networks & Communications, vol. 12, no. 4, pp. 19–39, 2020.

[26] J. Seetaram and P. S. Kumar, "An energy-aware genetic algorithm multipath distance vector protocol for efficient routing," 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), 2016.

[27] L. Malathi and R. K. Gnanamurthy, "Cluster-based hierarchical routing protocol for WSN with energy efficiency," International Journal of Machine Learning and Computing, vol. 4, no. 5, pp. 474–477, 2014.

[28] H. Fareen Farzana and S. Neduncheliyan, "Ant-based routing and QoS-effective data collection for Mobile Wireless Sensor Network," Wireless Networks, vol. 23, no. 6, pp. 1697–1707, 2016.

[29] M. Chaudhari, P. Koleva, V. Poulkov, and O. Asenov, "Multilayered distributed routing for power efficient Manet Performance," Wireless Personal Communications, vol. 97, no. 2, pp. 1729–1752, 2017.

[30] L. J., "Power Aware Energy Efficient Cluster based network coding algorithm for Dynamic Source Routing (PA-EECSNC DSR)," International Journal of Psychosocial Rehabilitation, vol. 24, no. 5, pp. 1742–1750, 2020.

Authors

Darshan B D received his BE degree in Electronics & Communication Engg. from Visvesvaraya Technological University, Belgaum, India, and his MTech degree in Digital Electronics & Communication Systems from Visvesvaraya Technological University, Belgaum, India. He is currently pursuing Ph.D. at the Department of Electronics and Telecommunication Engineering, Dr. Ambedkar Institute of Technology, Bangalore. His research interests include computer networking, communication engineering, Ad-hoc Networks, and Wireless Sensor Networks.

Prashanth C R received his BE degree in electronics, ME degree in digital communication, and a Ph.D. degree from Bangalore University, Bangalore, India. He is currently working at the Department of Electronics & Telecommunication Engineering and is Dean (Examinations) at Dr. Ambedkar Institute of Technology, Bangalore. His areas of interest are image processing, pattern recognition, biometrics, computer networks, communication engineering, device modelling, and Engineering Education. He has over 50 research publications in refereed International Journals and Conference-Proceedings.

How to cite this article:

Darshan B D, Prashanth C R, "Performance Analysis of Cluster-Based Dynamic Multipath Trust Secure Routing (DMTSR)-Protocol in Wireless Sensor Networks (WSNs)", International Journal of Computer Networks and Applications (IJCNA), 10(3), PP: 371-382, 2023, DOI: 10.22247/ijcna/2023/221891.