Telecommunication Systems (2024) 86:769–783
https://doi.org/10.1007/s11235-024-01170-1

A novel algorithm for the development of a multipath protocol for routing and energy efficient in IoT with varying density

Radwan S. Abujassar[1]

Accepted: 17 May 2024 / Published online: 1 June 2024

Abstract

Data transmission from sensor nodes is the biggest problem for IoT networks. Overusing communication power shortens node lifespans. Thus, network issues including QoS, security, network heterogeneity, congestion avoidance, reliable routing, and energy savings must be addressed. Routing protocols are essential for delivering data between organizations. Information gathering and consolidation require data aggregation to minimize traffic congestion, operating expenses, energy usage, and network lifespan. IoT data aggregation makes route planning dependable, energy-efficient, and difficult. Disjoint & Scalable Multipath Routing (D&SMR) is a new routing system developed using NS2 simulation. The method estimates delivery success using decision trees and neural networks. We evaluate characteristics such as (D&SMR) routing scheme predictability, node popularity, power consumption, speed, and location while training the model. Simulation results show that (D&SMR) outperforms a reliable routing system in terms of delivery success, lost messages, overhead, and hop count. The proposed hybrid routing method involves cluster construction and intra- and inter-cluster routing. The study found that (D&SMR) beats previous research in network resilience, packet transmission efficiency, end-to-end latency, and energy usage.

Keywords Internet of Things (IoT) · Energy efficiency · Network life time · Optimal path selection · Packet inquiry (PINQ)

1 Introduction

The Internet of Things (IoT) refers to a network that links a significant quantity of items. An object can be classified based on several characteristics. Firstly, it can be categorized as either virtual or physical. Second, an object is autonomous in terms of its decision-making and functioning. Third, it is capable of communicating with other devices. Fourth, an object is interactive and interoperable because it works with a variety of devices. Lastly, an object is flexible, as it can interact with any other object, regardless of location or service [1, 2]. However, from a technological standpoint, it is important to note that the IoT is not only a singular technology but rather a convergence of several networking components. Various technologies, including wireless sensor networks (WSN), radio frequency identification (RFID), smart ad hoc networks, vehicular ad hoc networks (VANET), wireless personal area networks (WPAN), wirelessfidelity networks (WIFI), and numerous more, have been developed. To clarify, the IoT currently comprises a vast and diverse network [3–6].

Within the IoT ecosystem, there exist several methodologies and protocols that provide effective communication and connectivity among items. In this context, one prominent strategy is the use of ad hoc mode [7, 8]. An ad hoc network refers to a transient infrastructureless peer-to-peer (p2p) network framework whereby each individual device undertakes the tasks of data collection, processing, storage, and transmission [9]. In the context of wireless communication, it is observed that devices establish connections with nearby devices through direct wireless transmissions. However, in cases where the distance between nodes exceeds the range of radio transmission, multi-hop transmissions are employed to facilitate communication between these nodes. In multihop communication, an entity that is transferring data uses additional entities as relays to expand the range of its transmission. Hence, a device depends on intermediary entities to construct pathways and transmit packets to their intended destinations. Ad hoc networks have several advantages, including efficient and rapid deployment,

✉ Radwan S. Abujassar
r.abujassar@aou.edu.kw

[1] Faculty Information Technology and Computing, Arab Open University-Kuwait, Alardiya Industrial, 830, 92400 Al-Ardiya, Kuwait

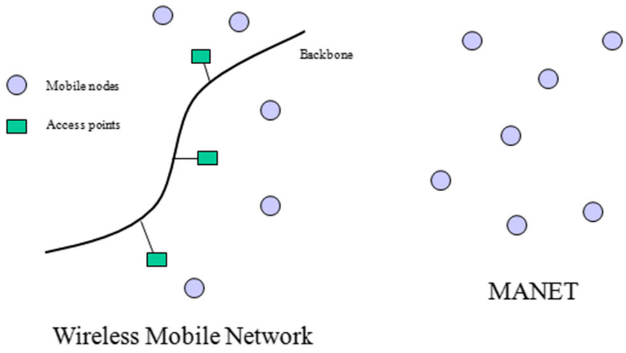

Fig. 1 Mobile Ad-hoc Network

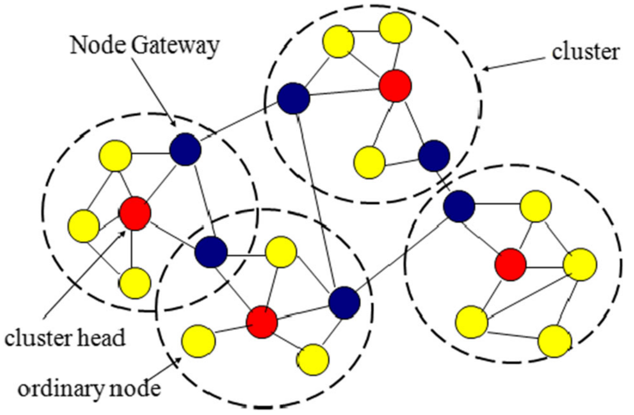

Fig. 2 Network Topologies with NCH

cost-effectiveness, adaptability, resilience, and support for mobility. Ad hoc networking is widely prevalent in many IoT applications, including but not limited to disaster rescue, cooperative intelligent transportation systems (CITS), e-health, logistics, military scenarios, and environmental sensing, among others. The user's text consists of three numerical references: [10, 11]. Furthermore, the ad hoc mode is a fundamental component of 5 G deployment modes, playing a crucial role in increasing the network's coverage area, maintaining service resilience, and improving the overall user experience [5, 12, 13].

Figure 1 illustrates the visual representation. Ad hoc networks are self-governing networks that function independently, or stub networks that establish connections with an existing fixed network. It is not advisable to solely depend on pre-existing infrastructure. Therefore, the absence of an access point is evidenced by the decentralized nature of the network, where each individual node functions as a router and assumes the role of forwarding packets on behalf of other nodes.

Figure 1 illustrates an exemplar of a mobile ad hoc network (MANET) in the context of the IoT. On the other hand, Fig. 2 portrays a scenario in which a satellite disseminates data simultaneously to several destinations inside a huge IoT network. The satellite facilitates the transmission and reception of communications, mostly directed towards a nearby smart device located on an aircraft or vessel. These messages serve the purpose of disseminating auditory and visual warnings. In the context of MANETs and the IoT, it is common for devices to often depart from and join the network or exhibit mobility, resulting in a dynamic alteration of the network's topology. This particular attribute presents a multitude of issues, particularly in the context of routing protocols, as self-organizing protocols become indispensable in these ecosystems [14, 15]. The essential components of the IoT are self-organization, information exchange, and information routing. To facilitate these operations, energy- and computation-limited devices employ routing protocols that prioritize optimization at the expense of security, in particular. Furthermore, due to the escalating proliferation of IoT devices and the recent advancements in interoperable protocols and middleware technologies, the dimensions of MANETs are continuously expanding. Consequently, these networks are becoming intricate compositions of diverse devices, facilitating the transmission of critical data. In addition, the multi-hop transmission paradigm operates on the assumption that devices exhibit complete cooperation and faithfully fulfill their roles in routing and forwarding. However, there are several motives, such as the goal of conserving energy, that might lead to nodes refraining from forwarding and routing packets. Certain entities with self-centered motives may exhibit a reluctance to engage in collaborative efforts. Conversely, in the case of individuals with malevolent intent, their primary goal is to disrupt the network and manipulate packet contents. These behaviors have a significant influence on the availability of connections in MANETs, leading to reduced connectivity and perhaps causing various packet transmission issues. In the context of multi-hop transmissions, it is important to note that each forwarding node has the potential to engage in a Man in the Middle (MITM) assault. Furthermore, as a result of the inherent spontaneity of the IoT and MANETs, devices possess the freedom to join or depart from the network at any given moment. Consequently, individuals who are newly introduced to the network lack pertinent information, rendering them susceptible to manipulation by malicious actors. Additionally, the process of joining and departing the network contributes to unstable connectivity, leading to heightened traffic and subsequent congestion. Furthermore, incidents necessitate updating the network topology.

2 The main contribution of this work

The contributions of this study are significant and noteworthy. The contributions of this study are summarized as follows:

- In this study, we provide a novel Disjoint & Scalable & Multipath Routing (D&SMR) algorithm and an adaptive multipath routing protocol specifically designed for IoT and MANETs.
- In this study, we present a mathematical assessment model that encompasses key attributes of a node, including mobility and uncooperative behaviors. This model is designed to be applicable to many ad hoc routing protocols.
- The proposed technique aims to improve node energy efficiency by optimizing the energy consumption of supplementary nodes in the provided topology that are not part of the primary path. In scenarios where nodes within a network experience migration or new nodes join, it is feasible to employ an alternative node situated on a distinct path from the primary one to alleviate any disturbances to the primary path.
- If any node inside a multipath or disjoint network becomes inactive or fails, our algorithm will initiate the creation of a new, distinct multipath or disjoint network prior to any network events taking place.
- The Internet of Things-enabled network (IOTN) is now a prominent field of research. While the IoT has been successfully used in several real-time applications, it is important to acknowledge that one significant limitation of IoT is its energy constraint. The management of energy limitations is achieved through the use of several energy-efficient strategies. Of all the actions conducted by the IOTN, routing stands out as the most energy-intensive task. In light of the aforementioned considerations, this paper presents a proposed route selection strategy that takes into consideration both the reliability score and the sensitiveness of the data. The nodes' reliability score is computed using evidence theory, and users are given the opportunity to specify the expected reliability score for data forwarding. According to the specified criteria, the route selection is prioritized based on the dependability score, with secondary consideration given to the route's length. The suggested technique's performance is evaluated using common performance indicators, and the findings demonstrate that the proposed approach produces superior results.
- The objective of this study is to provide many pathways from a given source to a destination, with the aim of mitigating the impact of a single point of failure.The optimal pathway selection is determined by taking into account the level of sensitivity associated with the data being conveyed. The calculation of route dependability entails the use of trust characteristics. The incorporation of the clustering idea has the effect of lowering energy usage and enhancing manageability.

The following portions of this work are organized in the follows manner: Sect. 3 presents a comprehensive review of the current body of research on safe routing inside the IoT framework. Section 4 of this article provides a thorough examination of the secure routing protocol that we have created. In addition, we give a mathematical model to evaluate the technique that we have suggested. Section 5 of this study evaluates the evaluation of our technique and the results that were obtained. To summarize, Sect. 6 functions as the concluding part of the study and also outlines potential areas for further research.

3 Background and related work

The issue of mobility challenges in IoT routing protocols has been the subject of substantial research in recent years, as evidenced by several scholarly works [16–19]. Numerous studies have consistently highlighted the absence of standardized protocols in the domain of reliable routing for IoT devices, with particular emphasis on ad hoc routing. Numerous previous studies [20–23] have focused on the development of routing protocols that prioritize improvements in routing efficiency rather than mesh topology connections, owing to the distinctive attributes and limitations of IoT devices. The IoTN has garnered considerable attention in academic studies because of its extensive potential for application in several areas such as healthcare, surveillance, item tracking, and environmental monitoring, among others. The author has provided a citation range, indicating that they are referencing multiple sources. An IoTN consists of a multitude of wireless sensors that possess the ability to detect, transmit, and analyze data. Wireless sensors are commonly put in regions that are inaccessible to humans, posing challenges in sensor management. The sensors are responsible for monitoring the surrounding environment and gathering the necessary data. The data that has been gathered is transmitted to a high-capacity node for additional data processing, facilitated by data transfer. Data transfer can occur through two distinct methods, namely direct and indirect data transmission. Data transmission encompasses two primary entities, namely the source and destination nodes. The source and destination nodes may alternatively be referred to as sender and receiver nodes. When engaging in direct data transmission, the source node is able to establish a direct connection with the destination node. Nevertheless, this is not feasible in all instances. The most prevalent kind of data transfer is an indirect method of communication. Indirect data transmission is the conveyance of data from a source to a destination via one or more intermediate nodes. The present methodology raises a number of concerns, as the forwarding behavior of the intermediary nodes remains uncertain, and there is a potential for malevolent intent on the part of the nodes. The aforementioned factor has an impact on the velocity, uniformity, and dependability of data transfer. Therefore, it is important to take into account all of these elements in order to guarantee the secure transfer of data.

Despite the manifold benefits of the IoT, including its capacity for self-governance, dynamic topology, cost-effectiveness, and ease of deployment, it continues to face limitations in terms of energy consumption, memory use, and processing capabilities [24]. Out of all the aforementioned concerns, the issue of energy restriction stands out as the most crucial problem that requires immediate attention. The utilization of a sensor's energy is facilitated by three modules, namely sensing, processing, and communication. Out of all the many capabilities, communication is the most energy-intensive. Routing is a pivotal procedure that facilitates communication between sensors, and it is often recognized as the most energy-intensive operation [25]. Due to the dynamic nature of the IoTN, determining optimal paths from the source to the destination is a significant challenge. Furthermore, the Index of Orthodontic Treatment Need IoT demonstrates active engagement in many real-time applications. Therefore, it is imperative for the routing mechanism to provide both reasonable data transmission time and enhanced dependability. In order to ensure low energy use, it is imperative that these fundamental standards are met. Attain satisfaction by using less energy. This article proposes a reliable route selection technique based on clustering, which effectively addresses the aforementioned difficulties while also ensuring energy efficiency. This study employs a cluster-based method due to its energy-saving potential. The essence of the clustering strategy is in the management of node members by the Node Cluster Head (NCH) node inside the clusters. The energy consumption of the NCH node is reduced, resulting in balanced energy consumption. This study ensures dependability by incorporating the fundamental principle of trust. The trust parameters play a crucial role in characterizing the characteristics of sensor nodes. Moreover, the present study aims to examine a specific facet of data security, focusing on user preferences. This study calculates numerous routes between the source and destination and ultimately selects the route with a higher dependability score as the final route. In their publication, the authors provide a novel methodology known as the multi-hop, adaptive, tree-based energy-balanced (DMATEB) method [26]. The algorithm determines the nearest node that possesses a substantial amount of remaining energy. The utilization of multi-hop routing, which incorporates the use of clusters, enhances both data collection efficiency and the overall lifespan of the network. The authors in [27] introduced the EACRA system as a means of mitigating the issue of periodic duplicate data transfer. The data is transferred from sensing devices in response to contextual changes, resulting in reduced energy consumption and message exchange. To assess their impact on network performance. According to the source, sensing devices are activated exclusively through heat application. The REERS system offers energy efficiency solutions for extensive implementations [27]. Efficient route selection for data aggregation is crucial in IoT contexts characterized by extensive connectivity. The REER framework takes into account both real-time and non-real-time situations. A routing system that prioritizes energy efficiency utilizes cost-effective paths to enhance the performance of real-time applications by reducing latency and optimizing energy consumption. In their study, they conducted data aggregation from designated monitoring stations, with a particular emphasis on optimizing the data gathering process. The scheme's algorithm aggregates data from both collecting and loading regions. The proposed methodology enhances the longevity of the network by evaluating the expense of the path between different regions and then transmitting the load of each sensing node. Researchers have found that mobile data collection sinks exhibit energy efficiency. Mobile devices can interact with data sensors to collect and combine data while navigating a specific path. This process involves many stages, including initialization, aggregation region selection, and path design, as outlined in reference [28]. The authors in [29] examine the energy and dynamic spectrum considerations associated with cluster-based routing. The implementation of self-distributed clustering techniques results in a reduction in power consumption and the generation of optimal clusters. The system possesses a greater number of co-sensing channels. The system transmits data across clusters by utilizing gateway nodes with higher energy levels and shared channels. It determines the head node by considering factors such as residual energy, channel availability, neighboring nodes, and distance from the sink. The proposed solution provides an efficient method to transfer data from the root to the sink. Achieving green routing in a wireless sensor network (WSN) poses significant challenges. Wireless sensor networks (WSNs) possess a finite amount of energy, which is allocated towards the execution of crucial activities in remote locations. Consequently, the availability of energy is diminished, thereby resulting in a reduction in the overall lifespan of the network.

In [30], double deep Q-learning dynamic arithmetic reinforcement learning (DQARL) is proposed for energy-efficient clustering and scheduling in reliable routing. The initial step suggests using Hunter Prey Optimization (HPO) to find the best head. The selection includes many fitness functions. In the second phase, duty cycling extends network life. This solution uses distributed scheduling to efficiently minimize sensor node energy usage. Schedulers examined sleep, listen, and transmit modes. Weighted Practical Byzantine Fault Tolerance (WPBFT) ensures stable routing and reduces packet transmission time in the third phase. This method selects the optimal source-cluster head path. This study investigates the power consumption of the compressor during the 20-minute start-up of the HRF under certain failure scenarios, including blockage of the 3-way valve and clogging of the capillary tube. The efficacy of these settings was evaluated in six failure scenarios. The compressor's power consumption is rapidly affected by both quantitative and qualitative changes in the refrigerant stream caused by these difficulties. The compressor power data clearly exhibited noticeable discrepancies in relation to the analyzed issues with refrigerant passage changes, serving as a signal for fault detection [31]. The author introduced a novel algorithm in the publication referenced as [32]. During the optimization process, several factors are carefully considered, including channel fade margin, cross-correlation and coherence time, spectral efficiency, interference level, power consumption, retransmission rate, access probability, and propagation delay. To improve the scheduling efficiency of the DE algorithm, many steps are meticulously designed: startup, mutation, crossover, fitness evaluation, selection for iteration evolution, and termination. The OMPS model assesses many measures including as latency, PDR, spectrum usage, interference level, energy efficiency, and the success rate of created paths.

The present technique employed by MDTA exhibits reduced energy consumption in comparison to prevailing energy-aware routing systems. Additionally, it evaluates the cost of data transmission in relation to the size of the network. The Agile data delivery system employs a very efficient data transmission mechanism that facilitates seamless communication between several nodes. The MDTA algorithm enhances the formulation of the root-to-sink path by considering both end-to-end latency and energy usage. This concept is applicable to a wide range of sensor and vehicle networks [33]. Wireless Sensor Networks (WSNs) encounter challenges in achieving energy-efficient data monitoring. The authors in [34] propose a scheduling approach that takes into account both sensor and network energy, with a focus on energy efficiency and quality. The effectiveness of data fusion is contingent upon the costs associated with data forwarding as well as the power capacity of the sensing nodes. The proposed methodology aims to reduce the number of active nodes while ensuring the integrity and dependability of the data. In their publication, the authors in [35] presented a routing system that utilizes location-based information to enhance the optimization of residual energy and network quality. The PEDAP algorithm was developed based on the concept of a near-optimal spanning tree with the objective of enhancing the lifetime of a network [36]. The localized PEDP system described in Reference [37] utilizes a distributed design, in contrast to other systems that adopt a centralized approach. In the seventeenth reference, the power-efficient gathering in sensor information systems (PEGASIS) protocol is described as a method that exclusively sends packets to neighboring nodes. This approach reduces the costs associated with the Low Energy Adaptive Clustering Hierarchy (LEACH) protocol. In [38], we propose a network structure called the delay-aware data collection network structure (DADCNS) in order to select tracks that have the least amount of latency in data gathering. This approach uses both top-down and bottom-up techniques to construct a hierarchical tree structure that governs the distances, rankings, and delays of the nodes.

In [39], the reduction of energy utilization is achieved by the implementation of a multi-hop algorithm that balances routing costs. The algorithm is capable of withstanding failures in both head and sensor nodes. In order to optimize energy dissipation, the SEED protocol is designed to minimize the occurrence of duplicate transmissions. However, it is not compatible with various sensor data. To tackle the issue of heterogeneous data trafficking and energy utilization in sensor nodes, an additional approach was introduced. In the LEACH Vice Cluster Head (L-VH) [15] protocol, a subordinate cluster head with the second highest energy level is responsible for managing the workload. The VH system does not operate simultaneously with the NCH system; rather, it remains in a dormant state until the CH system uses a sufficient amount of energy. Upon awakening, VH assumes the responsibilities previously assigned to NCH and thereafter fulfills CH's role. The reduction in the time required for selecting the next head and the decrease in the number of messages processed by VH for communication management are seen. The researchers in the referenced study propose a novel approach called Traffic and Energy-Aware Routing (TEAR) to identify nodes with high traffic and low energy consumption. In this particular scenario, TEAR does not offer redundant data filtering. The ETASA technique, which is a hybrid approach, offers enhanced load balancing by effectively managing the energy consumption of sensing devices. These devices are able to alternate between active and dormant states depending on considerations of energy levels and data transmission speeds. This paper aims to provide a routing method that prioritizes both route dependability and data sensitivity, drawing inspiration from previous research in the field. The majority of current literature focuses on providing security measures; however, it fails to address the ability for users to customize their route preferences. Nevertheless, this study enables the author to establish the anticipated reliability score of the route, taking into consideration the sensitivity of the data that is to be transferred. This concept serves to safeguard data against potential security risks while also mitigating energy use. Furthermore, the work demonstrates an increased quality of service (QoS). The subsequent section will provide an explanation of the functionality of the suggested strategy. A comparison has been shown in Table 1.

Table 1 Comparison with existing Protocol

Method	Strengths	Weaknesses
active trust [40]	High network stability is achieved by selecting reliable neighbors in secure transmission using a simple decision-making method	High communication cast, routing delay
Optimum routing [41]	Changes the major nodes and identifies the movement that is occurring on the primary nodes	High communication overhead, high time complexity
reliable routing [42]	Using a hierarchical architecture, taking into account energy efficiency and network security at the same time, taking into consideration the amount of energy that is still available in nodes while discovering new pathways, and employing hybrid cryptography to ensure that connections between nodes are properly protected	The failure is neither mitigated nor anticipated using this method. The design procedure lacks consideration for clustering, has a subpar trust mechanism, and is not scalable
Disjoint & Scalable Multipath Routing (D&SMR)	In the event of a disconnection, reroute the traffic, and there will be no additional cost associated with enabling UDP live streaming traffic. This will result in an improvement in power usage	There is a need for further enhancement in order to achieve higher speed and improved security during the exchange of data packets

4 Proposed an optimal rout selection strategy

Despite the multitude of advantages associated with the IoT, its primary issue is energy limitations. In the majority of real-time applications, sensors are deployed in hostile environments to facilitate the acquisition and analysis of data. As a result, periodic recharging or replacement of sensors is not feasible, potentially resulting in a node's premature failure. The prevention of this issue can only be achieved through the prudent utilization of the existing energy resources. Energy consumption is inversely proportional to the duration of network operation. This study aims to explore several strategies for minimizing energy usage, with a specific focus on the implementation of an energy-efficient and secure routing method. The energy consumption associated with the functioning of sensors is mostly attributed to the routing process, which surpasses all other processes in terms of energy utilization. Therefore, this study presents a routing policy for the IoT that aims to enhance energy efficiency and ensure trustworthiness. The present study employs the cluster model as a means to achieve the objective of enhancing energy efficiency. In this particular framework, the NCH has the responsibility of overseeing and controlling the activities of the node members. The NCH undergoes alteration within a designated time frame. In this manner, the utilization of energy in the sensor nodes is distributed evenly, resulting in a consistent energy consumption pattern. The Algorithm 1 illustrates a schematic representation of the overall flow of the proposed work.

When a source node desires to send a message to a destination node, the proposed methodology yields numerous potential pathways from the source to the destination. Furthermore, the user has the option to indicate the anticipated reliability of the chosen route. The selection process involves choosing the route that aligns with the desired level of trustworthiness from a set of available routes. As a result, this study takes into account the data's sensitivity and makes a modest contribution to the field of data security. This study primarily emphasizes the aspects of energy efficiency, route reliability, and a little consideration of data security. The subsequent section provides a comprehensive explanation of the proposed research.

4.1 Proposed D&SMR with its assumption

This paper is conducted based on specific assumptions, and the proposed methodology demonstrates superior performance when aligned with these assumptions. The assumptions are enumerated as follows:

- This study involves the implementation of a resilient mobile base station (BS) that is provided with a battery of substantial capacity.
- The nodes within the network stay immobile and have limited mobility at low speeds or with no movements.

- All nodes are equipped with information about their individual positions, notwithstanding the absence of Global Positioning System (GPS) functionalities. The network is composed of nodes that may be classified as either NCH or node members.
- The NCH possesses the capability to establish communication with both the Base Station (BS) and other Cluster Node Heads. The nodes possess the ability to communicate only with their respective cluster heads.

4.2 Topology formation with its NCH

Clustering's primary goal is to allocate a NCH for each cluster, ensuring that the NCH manages node members. The IoT lacks a centralized authority for overseeing node functionality, which is addressed by the introduction of a NCH to resolve this concern. Given the significant function played by the NCH, it is imperative that it exhibit qualities of trustworthiness and honesty. As a result, it is critical to observe node behavior and select the most appropriate nodes to serve as the NCH. It serves as the cluster's governing body. Therefore, it is imperative that the NCH organization maintain a high level of trustworthiness in its functioning. Nevertheless, the process of assessing the reliability of a node is more complex than it initially appears. While it is possible to quantify a node's trustworthiness, it is not advisable to rely solely on the trust evaluation provided by a single node. As a result, this study chose two distinct neighboring nodes to evaluate the sensor node's dependability score. The evidence theory is used to measure the nodes' dependability score. The use of evidence theory is advantageous because it does not require any prior knowledge of probabilistic ideas. The real reliability score is obtained by combining the reliability scores computed by two distinct neighborhood nodes; all notations are shown in Table 2. As denoted by Eq. (1), it is possible to categorize sensor nodes as either trustworthy or non-trustworthy, as well as reliable or non-reliable.

$$n : t = \{R, \bar{R}\} \tag{1}$$

The aforementioned Eq. (1) illustrates the potential trustworthiness of sensor node n, which may be classified as either trustworthy or non-trustworthy. This equation serves as a representation of this classification as following:

$$z = \{R\};\ \bar{z} = \{\bar{R}\};\ K = t \tag{2}$$

In the above equation, the symbol **R** represents the concept of reliability, whereas the symbol $\bar{\mathbf{R}}$ denotes non-reliability. Additionally, the symbol **K** represents the hypothesis pertaining to the potential reliability or non-reliability of the node. The probability function denoting the trustworthiness of the node is denoted by δ and may be expressed as follows 3 and 4:

Table 2 Math Notation

Notation	Definition
n	Nodes
t	Trust node
R	Reliable Node
$\bar{R}$	Non-Reliable Node
K	Represent all nodes Reliable OR non-Reliable
δ	Probability for node trust
T	Denoted to the shortest path
z	Denoted to Next Hop
$\bar{z}$	Denoted to Next Hop but in the main path
d	Distance
K_s	Nodes in the route from source

$$\begin{aligned} &z = \{R\};\ \bar{z} = \{\bar{R}\};\ K = t;\\ &\quad T1(z) = \delta;\ T1(\bar{z}) = 0;\ T1(K) = 1 - \delta; \end{aligned} \tag{3}$$

In this manner, the calculation of node reliability is performed, and the computation of dependability scores by two distinct nodes that are adjacent is expressed as follows. The equations provided below illustrate fictitious representation of the aforementioned events.

$$\begin{aligned} &z = \{R\};\ \bar{z} = \{\bar{R}\};\\ &\quad K = t;\ T1(z) = 0;\ T1(\bar{z}) = \delta;\ T1(K) = 1 - \delta; \end{aligned} \tag{4}$$

Equation (5) represents the proposal made by two neighboring nodes. The node has a significant degree of reliability. Equation (6) depicts the scenario when adjacent nodes acknowledge the existence of unreliability in the node. Ultimately, the node is classified as either dependable or undependable. The significance of qualities is critical in the decision-making process, and several approaches have been suggested to determine the appropriate weights.

$$\begin{aligned} &T1(z) \oplus T2(z) = \frac{1}{d} T1(z)T2(z)\\ &\quad + T1(z)T2(K) + T1(K)T2(z)\\ &\quad T1(\bar{z}) \oplus T2(\bar{z}) = \frac{1}{d} T1(\bar{z})T2(\bar{z})\\ &\quad + T1(\bar{z})T2(K) + T1(K)T2(\bar{z})\\ &\quad T1(K) \oplus T2(K) = \frac{1}{d} T1(K)T2(K) \end{aligned} \tag{5}$$

where **d** is given by

$$\begin{aligned} &d = T1(z)T2(z) + T1(z)T2(K) + T1(K)T2(z)\\ &\quad + T1(\bar{Z})T2(\bar{Z}) + \end{aligned}$$

$$T1(\bar{Z})T2(K) + T1(K)T2(\bar{z}) + T1(K)T2(K) \tag{6}$$

If there are numerous nearby nodes aside from the principal node, the following equation will be used to begin the computation of the ideal weight based on the most advantageous distance, using the **D&SMR** technique. As a result, the following equation explains how the primary approach determines the most favorable weight for the nearby elements. We made each cluster head pick the next alternative hop based on the minimum distance, as indicated: ∀ CH→ NextHop = min(distance$_{s-d}$) Until arriving at the destination, the route will serve as the foundation for the new routing table by creating the matrix_route as follows: M$_{Rout}$ equals min(∀ CH$_{nh}$ with minimum distance ∈ Cluster).

The node's dependability score ranges from zero to one, with a value of one indicating perfect reliability and a value of zero denoting complete unreliability. The presence of an intermediate value of 0.5 suggests that the node has limited reliability. When the base station (BS) encounters a cluster, all the nodes that are part of the cluster transmit the dependability score together with their identification to the BS. The base station (BS) selects the node with the highest dependability score and formally designates it as NCH. Following that, the remaining nodes transmit the JOIN request to the NCH and operate under the NCH's purview. As a result, the NCH is selected based on the identification of the most dependable node within the cluster. When the nodes inside a cluster need to transmit data to nodes in another cluster, they accomplish this by utilizing the NCH node. The NCH plays a vital role in the process of routing, as it is responsible for managing and maintaining two essential tables: the recent pathways database and the reliability scores table. When a network node intends to transmit a message to another node, it proceeds by forwarding the PINQ message to its designated next-hop controller. The PINQ message consists of three components: the source ID, the destination ID, and the predicted path reliability. The NCH verifies the destination identification (ID) and cross-references it with the most up-to-date path database. The current path table comprises the paths that have been most recently accessed. The table in question is designed to accommodate a maximum of 10 entities, with a mechanism in place to automatically remove older entities. This concept effectively preserves memory and facilitates the path-searching procedure. The routing method is outlined in the following manner: Assuming that the table includes the anticipated trajectory, the message's dependability score is evaluated. If a certain route meets the specified condition, it is chosen for the purpose of transmitting data. Conversely, in instances where the required path is absent from the database, the process of path discovery is initiated, leading to the retrieval of various pathways. The NCH systematically evaluates each path based on its node count and dependability score. The selection of a path is contingent upon the presence of a matching dependability score, which is mentioned in conjunction with the path request message. When the dependability score is lower than expected, the shortest path is disregarded. The dependability score for the given path is computed using the node's reliability score, which is measured on a scale from zero to one. A score of one signifies that the node is entirely trustworthy, while a score of zero indicates that the node is entirely unreliable. The intermediate value of 0.5 indicates that the node has a certain degree of reliability. When the base station (BS) encounters a cluster, all the nodes that are part of the cluster transmit the dependability score together with their identification to the BS. The base station (BS) selects the node with the highest dependability score and formally designates it as the NCH. Subsequently, the remaining nodes transmit the JOIN request to the NCH and operate under the CH's purview. As a result, the cluster selects the most dependable node, the NCH, as shown in Algorithm 1 (Table 3).

Algorithm 1 Algorithm for NCH

```
$Creatalltoplogiesthenselect NCH$
$count = 0; Min = 100 sec$
$(NCH \rightarrow selectedBasedonLSDBInfo.History)$
$countExchangeInquiryPacketsoutboundfromallnodes$
$AlladjacentNodes \leftarrow\notin mainpath(NCH\&Dest)$
while $NH\neg mainRoute$ do
  $getNH\_i\_d$
  $count++$
  $Computethereliableallnodesnotinthemainpath$
   $K\_r = NH(K\_r) + NNH(K\_r)$
   if $K\_r > count$ then
     $DeclaretheKistheNCH$
   end if
   if $rout[K][NH_{id}] = adj$ and $rout[K][NH_{id}] \neq PrimaryAdj$ then
     $NextHop[K] = ara_rout[K][NH]$
     $i \leftarrow ID + 1$
     $FomringRoute[K][NH] = rout[NextHop[NH\_i\_d]][Adjacent]$
   end if
   $P\_r = (NCH, V\_i), (NCH, D)$
   $NCH = Find(ADJ\_LeadTo\_Dest(D)$
   $\notin MNH, LongDistance)$
   $Check\_its\_K(Adjacent\_Node)$
   $Head\_Path\_to\_Destination = Head- > V\_i = (V\_i + 1, D)$
   $V\_i\_Adjacnet\_LabeledAsAvailable = (P\_rout) \notin Destination\cap$
   $\forall AdjacentsourroundedAs\_alt = Head- > V\_i- > Destination$
end while
$returnNode\_has\_ADJWithLowDist\_BuildPath;$
```

Table 3 Algorithm Notation and Definition

Notation	Definition
NH	Next Hop
NNH	Next Next Hop
ADJ	Adjacent Node
Dest	Destination
alt	Alternative Node
S	Source
NCH	Node Cluster Head
PINQ	Packets Inquiry

5 Simulation experiment

An evaluation was conducted using network simulation to assess the effectiveness of the upgraded D&SMR protocol in NS2-simulated networks with both high and low node densities. The results derived from comparing the simulation of the D&SMR protocol with other well-established protocols, such as active trust [40], optimum routing [41], and reliable routing [42], The NS2 simulation demonstrated the potential of IoT technology to improve nodes' preparedness and agility in various connection situations. Radio propagation required a transmission capacity of 0.28 watts. Within a radius of 250 ms, the technology allowed nodes to send and receive data packets. To enable wireless transmission of multimedia files, the researcher included IEEE 802.11b technology at both the physical and data-link layers. The NS2 utilized the Way-Point random mobility paradigm inside a roaming area measuring 1000 x 800m^2. During the simulation, clusters of nodes emerged. The predicted beginning velocity of 1 m/s was moderately low. However, the effects of this velocity selection will become apparent and substantial in future research and relationships. Each simulation lasted for a length of 600 s. The experimental approach involved conducting one hundred trials, followed by the calculation of the mean value. The maximum length of a packet was 1024B, although its capacity was restricted to 512 bytes. The bit rate was set to 2Mb/sec. It is widely known that devices in an ad hoc configuration network have the ability to share a wireless connection. The first simulated scenario consisted of an evenly distributed density of 200 to 300 nodes in each cluster location. Throughout the experiment, a steady data transmission rate of 512B per second was observed between the source and destination nodes. The next part presents the results of the simulation, which are depicted visually in the form of line graphs. The specific characteristics of the diagrams are provided in Table 4. The packet loss ratio is determined by dividing the number of discarded packets by the total number of sent packets. The average end-to-end latency is a statistical measure that calculates the average time it takes for a data packet to be transmitted and successfully received. Before evaluating the performance effects of network topologies on the calculation of a backup path in MANET, it is essential to determine the network components that could affect the quality of service (QoS) of the video data being sent. This research specifically examines three distinct qualities. This study aims to elucidate the impacts of video traffic strategies by specifically examining three key attributes. To evaluate the influence of node density, it is critical to recognize that higher densities are associated with longer lifespans compared to lower or intermediate densities. This difficulty occurs because the latter's capacity to accurately detect and maintain new pathways decreases when the nodes spread out into different clusters, increasing the chances of creating a disconnected structure. When there is less movement, regions consisting of nodes demonstrate increased stability, which allows for the provision of services for longer periods of time. After dividing the networks into many clusters, we conducted measurements to assess the packet delivery ratio, throughput, latency, and power consumption.

5.1 Performance and analyses evaluation

In the simulation conducted, there were a total of 200 nodes when there was mobility and 300 nodes for a stable network. All nodes were distributed inside a square space of 1000 x 800^2. The distribution of all nodes is uniform and random. The placement of the sink node is positioned in the centroid of the area. Each node in the network is subject to a random waypoint mobility (RWM) model, where the speed of the nodes ranges from 0 to 10 m/s [43]. The simulation parameters have been described in Table 4. In this study, we conducted a comparative analysis of D&SMR in relation to active trust, reliable routing, and the optimum path. The evaluation was based on many performance metrics, including PDR, energy consumption, average end-to-end (AE2E) latency, network lifespan, network energy consumption, cluster formation time, and cluster lifetime.

- **CLUSTER Life TIME VS. NUMBER OF NODES**
  The cluster building time refers to the processes of cluster formation and NCH selection. A prolonged duration for cluster setup implies that the procedure exhibits a high level of complexity. Figure 3 demonstrates the influence of node density on the duration required for clustering construction. As we can see, the proposed algorithm has reduced the time by around 30% compared with reliable routing and 5% to 10%. The D&SMR algorithm was also used for NCH selection, relying on the number of nodes in each cluster and the best energy for the nodes. Furthermore, based on the measurement distance, the sink node will be in the center of all cluster nodes.

Table 4 Simulation Parameter

Parameter	Value
Simulation Time	600 sec
Simulator	Network Simulator (NS2)
Number of Nodes	200–300
Wireless Channel	Unit Disk Graph Medium (UDGM)
Max. range	250 m
Roaming area	1000 X 800 m^2
Min. Speed	0 m/s
Max. Speed	up to 10 m/s
Mobility model	Random WayPoint Mobility
Threshold Value	1Mb
Initial Energy of Nodes	2J
Packet Size	512B
Propagation Model	Free-Space
Compared Routing Protocol	Reliable Routing,Active Trust, Optimal Routing
Transport Protocol	UDP
CBR rate	2Mbps

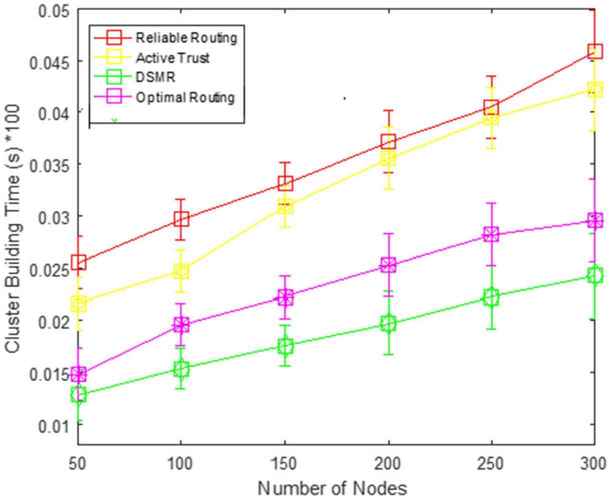

Fig. 3 Cluster Building Time

In the case of a large number of nodes, the duration required for cluster formation increases significantly across the majority of clustering methods. In the D&SMR framework, the developed PINQ packet was employed to effectively decrease the clustering construction time. The duration between cluster development and dissolution is an indicator of its longevity and a significant determinant of network energy consumption. Within the context of D&SMR, it is observed that a node possessing a greater fitness value assumes the role of the NCH. In the present study, we examine residual energy as a primary determinant for NCH selection. The cluster lifetime was defined in Eq. (7).

$$NCH^{LF} = \frac{Energy(i)}{E_{total}} \tag{7}$$

Once the energy of a node drops below a certain threshold, the algorithm must start the process of selecting the NCH. In the topology, the variable **i** represents the energy level of each node. A shorter cluster lifespan results in higher energy usage because it necessitates re-clustering and NCH selection. Figure 4 depicts a clear inverse relationship between node densities and cluster longevity, suggesting that as node densities increase, cluster duration decreases. The frequent alterations in network design, resulting from the movement of nodes, have an adverse impact on the longevity of the cluster, leading to a reduction in its length. The diagram illustrates the energy usage generated by the transmission and reception processes at both the source and intermediate nodes that have successfully delivered the packet. It is important to note that with D&SMR, The network displays lower energy consumption in comparison to other networks. Reliable routing, active trust, and optimal routing use energy by transmitting and receiving packets that are then lost due to buffer overflow and congestion. The route continues without achieving a successful delivery.

- **PDR VS. NUMBER OF NODES**

The protocol's performance was investigated by manipulating the network's node density. In this investigation, we varied the number of nodes within the range of 20 to 200. The node density has a substantial impact on the PDR. Because of their low density, the nodes frequently encounter link disconnection problems, resulting in a

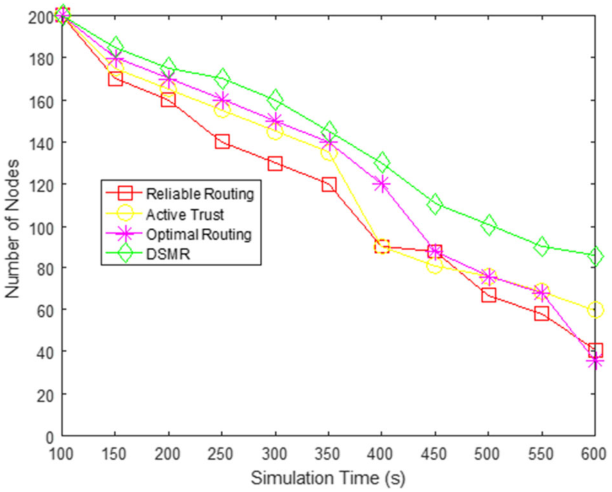

Fig. 4 Life Time

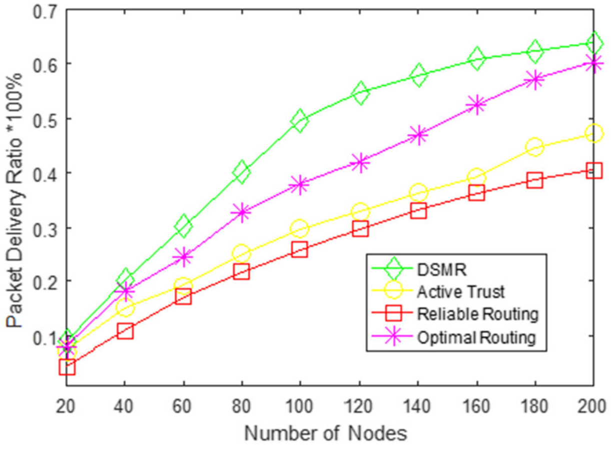

Fig. 5 Packet Delivery Ratio

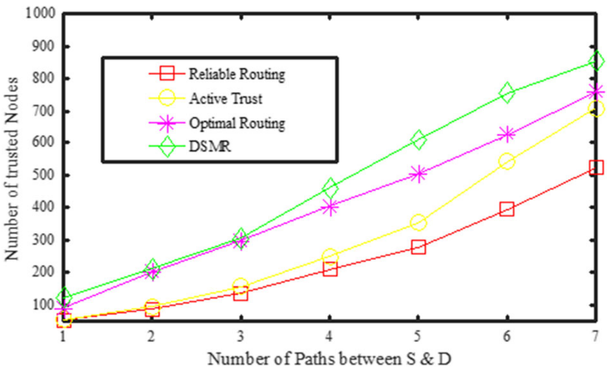

Fig. 6 Packet Over All Ratio Received

decrease in the PDR. The Fig. 5 illustrates the aggregate number of packets lost per second in the network due to buffer overflow and loss in the wireless channel. Considering the aforementioned variables, it is not unexpected that D&SMR experiences a significantly lower rate of packet loss at the buffer. The D&SMR technique employs the modified PINQ packet policy, whereas active trust, dependable routing, and optimal routing lack a mechanism for adapting the transmitting rate. However, the quantity of lost packets stays constant. The levels of inactive trust, dependable routing, and optimal routing are higher in comparison to D&SMR, which has an impact on the received PDR. The graphic illustrates that D&SMR, active trust, reliable routing, and optimal routing transmit 2.47, 5.41, and 25.91 packets per second, respectively. Furthermore, the numerical value The packet loss rate per second for active trust, reliable routing, and optimal routing is 0.32, 0.44, and 0.56, respectively. After increasing the number of nodes, there is a significant increase in the PDR. Regarding all the procedures, Our proposed D&SMR demonstrates improved performance when compared to active trust, reliable routing, and optimal routing strategies. This is because we have taken into account the effectiveness of the two-hop neighbor-based clustering strategy, which is superior to the one-hop neighbor-based clustering approach. Neighbor information improves the overall understanding of the network.

The results illustrated in Fig. 6 demonstrate that an increase in the number of nodes inside each cluster results in a proportional increase in the availability of paths between the source and destination. Consequently, the network's performance is affected.

- **AE2E DELAY VS. NUMBER OF NODES**

Figure 7 illustrates the end-to-end latency, which represents the duration from when a packet is created at the source application to when it is successfully received at the destination application. D&SMR has a reduced end-to-end latency in comparison to active trust, reliable routing, and optimal routing. D&SMR initially scans for an uncongested area around the forward packets. If congestion or other issues persist, the quantity of packets injected into the network is decreased by lowering the sending rates of the nodes. As a result, the buffer for the neighboring nodes can quickly accept and transmit packets without experiencing significant buffer delays. However, active trust, reliable routing, and optimal routing experience significant delays due to the periodic increase and decrease of exchanged packets in each topology, which is influenced by the network conditions. This process persists when there is congestion. As a result, the packets experience significant delays in the nodes' buffers. While active trust routes packets down less crowded channels, it does not implement a mechanism to decrease the sending speeds of nodes when buffer

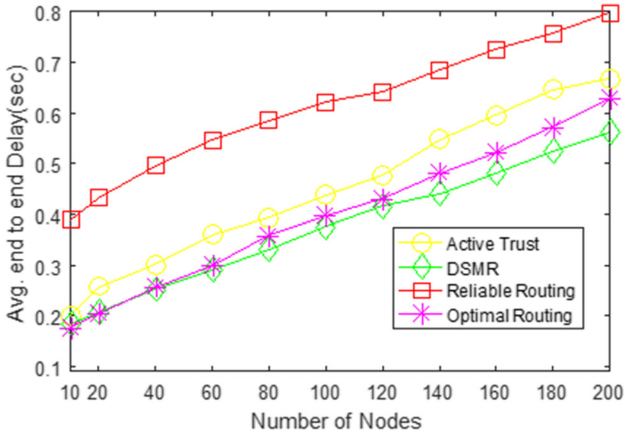

Fig. 7 End to End Delay

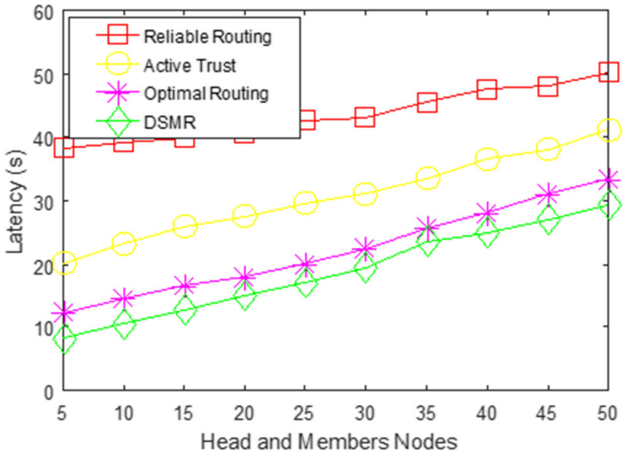

Fig. 8 Latency analysis

drops still happen. As a result, packets will encounter significant delays from one end of the network to the other if the buffers are consistently filled. There is a clear positive correlation between the density of nodes and the latency of AE2E. This is because the task of determining the node's location and creating routes becomes time-consuming when the nodes are moving. Implementing our two-hop neighbor strategy leads to a decrease in the latency of node AE2E when compared to clustering and routing protocols that rely on one-hop. Within the framework of D&SMR, the application of NCH in clustering is used to improve the stability of clusters.

- **NODES LATENCY vs ENERGY CONSUMPTION**

The experimental findings demonstrate the effectiveness of the suggested technique, as evidenced by the observed performance. Additionally, a latency analysis of the proposed approach is presented in Fig. 8. The suggested technique has a higher packet delivery rate because it considers the trustworthy path rather than only prioritizing the shortest route. Trustworthiness is prioritized above the length of the journey. The suggested work demonstrates an enhanced packet delivery rate. The latency analysis assesses the average delay experienced by each individual technique. Minimizing latency is crucial in order to increase the quality of service (QoS). This study demonstrates low latency due to the selection of reliable sources and the utilization of the most efficient route. The presence of malicious nodes along the route could potentially cause packet-forwarding delays. This study adopts a trustworthiness-based approach, resulting in reduced delay.

Figures 9 and 10 demonstrate the relationship between energy usage and node density fluctuations. The D&SMR protocol demonstrates a lower energy consumption, saving around 35% in comparison to other protocols that are

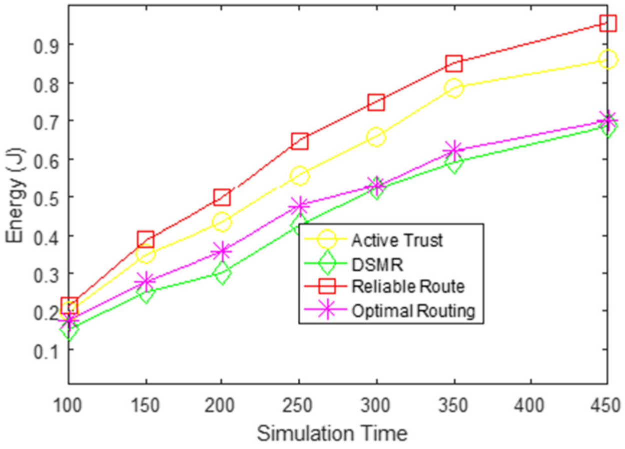

Fig. 9 Energy consumption vs. number of nodes

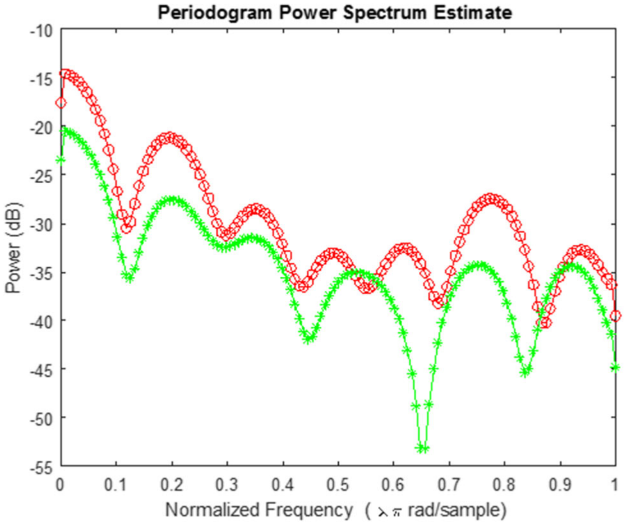

Fig. 10 Power consumption for the D&SMR within simulation

equivalent in nature. The consideration of node energy is deemed essential in the processes of clustering, NCH selection, and routing, owing to its impact on achieving an optimal number of clusters. In the suggested methodology, we employ an analytical optimization technique to determine the optimal number of clusters for our network's spectrum power analysis. This optimization process is carried out throughout the simulation, as shown in Fig. 10. This is because the next alternative hop will be in sleep mode until a failure or any disconnection occurs during the transmission. The relationship between total energy consumption and round work may be observed in the context of minimizing the number of single-node clusters, leading to reduced energy consumption. Figure 10 illustrates the declining trend of the node's residual energy rate. The D&SMR protocol has a larger residual energy compared to other protocols due to its ability to disperse energy use among nodes, resulting in a slower depletion of energy in individual nodes. Hence, in the context of D&SMR, a greater number of nodes have a higher likelihood of survival in comparison to alternative techniques.

The graph depicted in Fig. 9 showcases the rate of energy consumption among the nodes. A negative correlation exists between the lifespan of a network and its energy use. A network's energy consumption is inversely proportional to its longevity, meaning that a longer lifespan is correlated with lower energy consumption. After thorough analysis, it has been concluded that the energy consumption rate linked to the proposed methodology is significantly lower than the already utilized approaches. Selecting the most efficient route is crucial for reducing energy use. When a node demonstrates slow packet forwarding, as is frequently observed with malicious nodes, it leads to higher energy consumption. However, our analysis chooses the path based on dependable nodes, as indicated by Eq. (8).

$$K_s(Rout_i) = \frac{K_s}{\forall nodes} \tag{8}$$

Integrating the concept of clustering helps reduce energy use even more. The recommended work's minimal energy consumption results in a significant improvement in the network's durability. Overall, the simulations demonstrate that the D&SMR algorithm outperforms the active trust, reliable routing, and optimal routing approaches to a substantial degree. Furthermore, it is D&SMR clearly outperforms active trust, reliable routing, and optimal routing in terms of energy usage, with average improvements of more than 19.36%, 28.02%, 30.07%, 31.97%, 40.2%, 52.58%, and 62.35%, respectively, during the whole simulation period.

6 Conclusion and future work

This article presents a method for choosing a way that considers both the reliability of the road and the level of sensitivity of the data being transmitted. Certain data possesses a higher level of sensitivity, which in turn raises the probability of potential modifications or removals taking place throughout the routing process. Each individual pathway has the capacity to contain nodes that are either reliable or malicious. The presence of malevolent nodes might result in unfavorable behaviors, rendering the route that incorporates them unsuitable for sending extremely sensitive data. This study introduces a new method for choosing a path that allows users to designate the desired level of dependability for the chosen path. The dependability score is calculated on a scale ranging from 0 to 1. The path that satisfies the specified dependability score is further optimized based on its duration. The execution of these procedures is carried out using a NCH with the objective of conserving energy. This concept efficiently preserves energy and maximizes the lifespan of the network. The objective of this study is to investigate the capacity of mobile nodes to improve energy efficiency. Our future work will focus on integrating D&SMR with other IoT technologies, including edge computing and 5 G/6 G networks. We will also modify or improve the algorithm to tackle the issues posed by next-generation IoT systems. The clustered design of the head node will result in further power savings. It will also facilitate the expansion of the network to accommodate up to 1000 nodes. Furthermore, security measures will be enhanced to prevent any malicious packets or assaults during transmission.

Funding No Funding.

Data and materials availability The datasets generated during and/or analysed during the current study are available from the corresponding author on reasonable request.

Declarations

Conflict of interest We certify that there is no actual or potential Conflict of interest in relation to this article.

Ethical approval I have approved there is no Conflict of interest for this study.

References

1. Ghamari, M., Janko, B., Sherratt, R. S., Harwin, W., Piechockic, R., & Soltanpur, C. (2016). A survey on wireless body area networks for ehealthcare systems in residential environments. *Sensors, 16*(6), 831.
2. Crosby, G. V., Ghosh, T., Murimi, R., & Chin, C. A. (2012). Wireless body area networks for healthcare: A survey. *International Journal of Ad Hoc, Sensor & Ubiquitous Computing, 3*(3), 1.

3. Arafat, M. Y., & Moh, S. (2022). JRCS: Joint routing and charging strategy for logistics drones. *IEEE Internet of Things Journal, 9*(21), 21751–21764.
4. Mu, J., Wei, Y., Ma, H., & Li, Y. (2020). Spectrum allocation scheme for intelligent partition based on machine learning for inter-WBAN interference. *IEEE Wireless Communications, 27*(5), 32–37.
5. Al-Turjman, F. (2017). Energy-aware data delivery framework for safety-oriented mobile IoT. *IEEE Sensors Journal, 18*(1), 470–478.
6. Aledhari, M., Razzak, R., Qolomany, B., Al-Fuqaha, A., & Saeed, F. (2022). Biomedical IoT: Enabling technologies, architectural elements, challenges, and future directions. *IEEE Access, 10*, 31306–31339.
7. Dian, F. J., Vahidnia, R., & Rahmati, A. (2020). Wearables and the internet of things (IoT), applications, opportunities, and challenges: A survey. *IEEE Access, 8*, 69200–69211.
8. Barakah, D.M., & Ammad-Uddin, M (2012). A survey of challenges and applications of wireless body area network (WBAN) and role of a virtual doctor server in existing architecture. In *2012 Third international conference on intelligent systems modelling and simulation*, IEEE. pp. 214–219.
9. Qu, Y., Zheng, G., Ma, H., Wang, X., Ji, B., & Wu, H. (2019). A survey of routing protocols in WBAN for healthcare applications. *Sensors, 19*(7), 1638.
10. Li, S., Kim, J. G., Han, D. H., & Lee, K. S. (2019). A survey of energy-efficient communication protocols with QoS guarantees in wireless multimedia sensor networks. *Sensors, 19*(1), 199.
11. Rani, S., Talwar, R., Malhotra, J., Ahmed, S. H., Sarkar, M., & Song, H. (2015). A novel scheme for an energy efficient internet of things based on wireless sensor networks. *Sensors, 15*(11), 28603–28626. https://doi.org/10.3390/s151128603
12. Yadav, R. N., Misra, R., & Saini, D. (2018). Energy aware cluster based routing protocol over distributed cognitive radio sensor network. *Computer Communications, 129*, 54–66. https://doi.org/10.1016/j.comcom.2018.07.020
13. Cengiz, K., & Dag, T. (2017). Energy aware multi-hop routing protocol for WSNs. *IEEE Access, 6*, 2622–2633.
14. Xiao, K., Wang, R., Deng, H., Zhang, L., & Yang, C. (2019). Energy-aware scheduling for information fusion in wireless sensor network surveillance. *Information Fusion, 48*, 95–106.
15. Altowaijri, S. M. (2022). Efficient next-hop selection in multi-hop routing for IoT enabled wireless sensor networks. *Future Internet, 14*(2), 35.
16. Moussa, N., Hamidi-Alaoui, Z., & El Belrhiti El Alaoui, A. (2020). ECRP: An energy-aware cluster-based routing protocol for wireless sensor networks. *Wireless Networks, 26*, 2915–2928.
17. Mehmood, A., Mauri, J. L., Noman, M., & Song, H. (2015). Improvement of the wireless sensor network lifetime using leach with vice-cluster head. *Ad Hoc and Sensor Wireless Networks, 28*(1–2), 1–17.
18. Shagari, N. M., Idris, M. Y. I., Salleh, R. B., Ahmedy, I., Murtaza, G., & Shehadeh, H. A. (2020). Heterogeneous energy and traffic aware sleep-awake cluster-based routing protocol for wireless sensor network. *IEEE Access, 8*, 12232–12252.
19. Salunkhe, S. P.,& Patil, H. D. (2016). Delay efficient authenticated anonymous secure routing for MANETs. *International Journal of Computer Applications*, **148**(4).
20. Sbeiti, M., Goddemeier, N., Behnke, D., & Wietfeld, C. (2015). PASER: Secure and efficient routing approach for airborne mesh networks. *IEEE Transactions on Wireless Communications, 15*(3), 1950–1964.
21. Babbitt, T. A.,& Szymanski, B. K. (2016). Trust based secure routing in delay tolerant networks. In *2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, IEEE. pp. 542–547.
22. Kardaş, S., Celik, S., Arslan, A., & Levi, A. (2013). An efficient and private RFID authentication protocol supporting ownership transfer. In *Lightweight cryptography for security and privacy: Second international workshop*, LightSec 2013, Gebze, Turkey, May 6-7, 2013, Revised Selected Papers 2, Springer. pp. 130–141.
23. Saxena, D., & Patel, P. (2023). Energy-efficient clustering and cooperative routing protocol for wireless body area networks (WBAN). *Sādhanā, 48*(2), 71.
24. Lalitha, S., Sundararajan, M., & Karthik, B. (2023). Reliable multipath route selection strategy based on evidence theory for internet of things enabled networks. *Measurement: Sensors, 27*, 100795.
25. Raja Basha, A. (2022). A review on wireless sensor networks: Routing. *Wireless Personal Communications, 125*(1), 897–937.
26. Haseeb, K., Saba, T., Rehman, A., Ahmed, Z., Song, H. H., & Wang, H. H. (2022). Trust management with fault-tolerant supervised routing for smart cities using internet of things. *IEEE Internet of Things Journal, 9*(22), 22608–22617.
27. Chandnani, N., & Khairnar, C. N. (2022). An analysis of architecture, framework, security and challenging aspects for data aggregation and routing techniques in IoT WSNs. *Theoretical Computer Science, 929*, 95–113.
28. Reddy Yeruva, A., Saleh Alomari, E., Rashmi, S., Shrivastava, A., Kathiravan, M., & Chaturvedi, A. (2023). A secure machine learning-based optimal routing in ad hoc networks for classifying and predicting vulnerabilities. *Cybernetics and Systems*, 1–12.
29. Vellela, S. S.,& Balamanigandan, R. (2023). Optimized clustering routing framework to maintain the optimal energy status in the WSN mobile cloud environment. *Multimedia Tools and Applications*, 1–20.
30. Kaythry, P., Kishore, R., & Avinash, E. (2024). Reliability based multistage ARQ for wide area wireless sensor networks. *Journal of Engineering Science and Technology, 19*(2), 374–389.
31. Papachary, B., Arya, R.,& Dappuri, B. (2024). Power-aware QoS-centric strategy for ultra reliable low latency communication in 5G beyond wireless networks. *Cluster Computing*, 1–14.
32. Dasari, R., & Venkatram, N. (2024). Optimizing multichannel path scheduling in cognitive radio Ad HoC networks using differential evolution. *Scalable Computing: Practice and Experience, 25*(2), 1199–1218.
33. Rocha, D., Teixeira, G., Vieira, E., Almeida, J., & Ferreira, J. (2023). A modular in-vehicle c-its architecture for sensor data collection, vehicular communications and cloud connectivity. *Sensors, 23*(3), 1724.
34. Kaur, P., Kaur, K., Singh, K., Bharany, S., Almazyad, A. S., Xiong, G., Mohamed, A. W., Shokouhifar, M., & Werner, F. (2023). Acoustic monitoring in underwater wireless sensor networks using energy-efficient artificial fish swarm-based clustering protocol (EAFSCP).
35. Wang, H., Li, Y., Zhang, Y., Huang, T., & Jiang, Y. (2023). Arithmetic optimization AOMDV routing protocol for FANETs. *Sensors, 23*(17), 7550.
36. Manoharan, J. S. (2023). A metaheuristic approach towards enhancement of network lifetime in wireless sensor networks. *KSII Transactions on Internet & Information Systems*, **17**(4).
37. Hadwa, S. M., Ghouraba, R. F., Kabbash, I. A., & El-Desouky, S. S. (2023). Assessment of clinical and radiographic efficiency of manual and pediatric rotary file systems in primary root canal preparation: A randomized controlled clinical trial. *BMC Oral Health, 23*(1), 687.
38. Ullah, S., Saleem, A., Hassan, N., Muhammad, G., Shin, J., Minhas, Q. -A.,& Khan, M. K. (2023). Reliable and delay aware routing protocol for underwater wireless sensor networks. *IEEE Access*.
39. Gopi, B., Ramesh, G., & Logeshwaran, J. (2022). The fuzzy logical controller based energy storage and conservation model to achieve maximum energy efficiency in modern 5G communication.

ICTACT Journal on Communication Technology, 13(3), 2774–2779.

40. Sahu, M., Sethi, N., & Das, S. K. (2022). Secure data transmission in wireless sensor networks with secure system for identification of trusted route with node behavior analysis. *Revue d'Intelligence Artificielle*, **36**(2).
41. Gupta, S. K., & Singh, S. (2022). Survey on energy efficient dynamic sink optimum routing for wireless sensor network and communication technologies. *International Journal of Communication Systems, 35*(11), 5194.
42. Abbas, G., Ullah, S., Waqas, M., Abbas, Z. H., & Bilal, M. (2022). A position-based reliable emergency message routing scheme for road safety in VANETs. *Computer Networks, 213*, 109097.
43. Valle, M. S., Casabona, A., Sapienza, I., Laudani, L., Vagnini, A., Lanza, S., & Cioni, M. (2022). Use of a single wearable sensor to evaluate the effects of gait and pelvis asymmetries on the components of the timed up and go test, in persons with unilateral lower limb amputation. *Sensors, 22*(1), 95.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Radwan S. Abujassar currently holds the position of Associate Professor at the Faculty of Information Technology and Computing at the Arab Open University-Kuwait, an institution associated with the prestigious University of OU in the United Kingdom. Dr. Radwan is currently the faculty's local dean and a member of the AOU-Kuwait scientific committee. Dr. Radwan earned his bachelor's degree in computer science from Applied Science University in Amman, Jordan, in 2004, and then acquired an M.Sc. degree from the New York Institute of Technology in 2007. In 2012, Dr. Radwan earned a Ph.D. from the University of Essex, UK, with a specialization in IP recovery in IGP and MANET networks in the field of computer and electrical studies. He is interested in studying network architecture and control systems, particularly focusing on routing protocols and IoT.