doi:10.20944/preprints202001.0304.v1

A Gray System Theory Based Multi-Path Routing Method for Improving Network Lifetime in Internet of Things Systems

Meysam Zarei[1] . Mohammadreza Soltanaghaei [2]

Abstract Internet of things (IoT) is a network of smart things. This indicates the ability of these physical things to transfer information with other physical things. IoT has introduced various services and daily human life depends on its reliable and accessible operation. The characteristics of these networks, such as topology dynamicity and energy constraint, challenges the routing problem in these networks. Previous routing methods could not achieve the required performance in this type of network. Therefore, developers of this network designed and developed specific methods in order to satisfy the requirements of these networks. One of the routing methods is utilization of multi-path protocols which send data to its destination using routs with separate links. One of such protocols is AOMDV routing protocol. AOMDV protocol is a multi-path protocol which uses multiple different paths for sending information in order to maintain the network traffic balance, manage and control node energy, decrease latency, etc. In this paper, this method is improved using gray system theory which chooses the best paths used for separate routes to send packets. To do this, AOMDV packet format is altered and some fields are added to it so that energy criteria, link expiration time, and signal to noise ratio can also be considered while selecting the best route. The proposed method named GSTMPR-IoT is introduced which chooses the routs with highest rank for concurrent transmission of data, using a specific routine based on the gray system theory. In order to evaluate and report the results, the proposed GSTMPR-IoT method is compared to the EECRP and AOMDV approaches with regard to throughput, packet delivery rate, end to end delay, average residual energy, and network lifetime. The results demonstrate the superior performance of the proposed GSTMPR-IoT compared to the EECRP and AOMDV approaches.

Keywords Internet of Things (IoT) . Gray System Theory. Multi-Path Routing . GSTMPR-IoT

✉ Meysam Zarei
Sm.zarei@khuisf.ac.ir

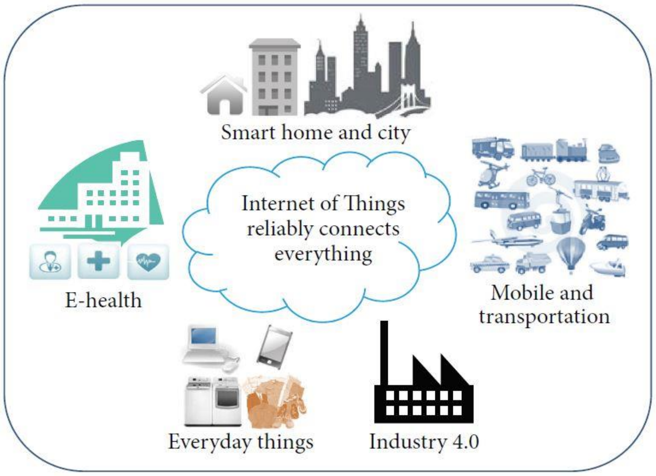
✉ Mohammadreza Soltanaghaei *
Mersa6@yahoo.com

[1] Department of Computer Engineering, Islamic Azad University, Isfahan (Khorasgan) Branch, Isfahan, Iran
[2] Department of Computer, Isfahan (Khorasgan) Branch, Islamic Azad University, Isfahan 81595-158, Iran

1 Introduction

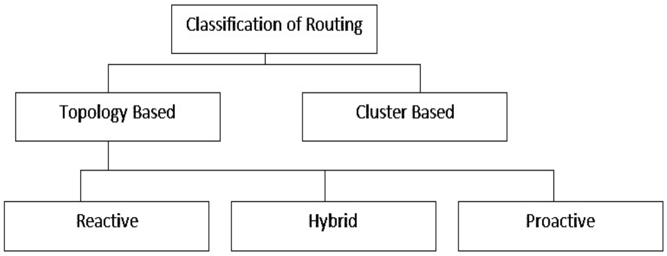
Recently, the demands of Internet of Things (IoT) keep growing. In the beginning, wireless sensor network (WSN) enables ubiquitous sensing technologies. As the WSN technology evolves, the proliferation and application of these sensing devices create the Internet of Things (IoT) [1, 2]. IoT is the next revolution, where the interconnection among smart objects creates an intelligent environment. It is estimated and expected to reach 24 billion IoT devices by 2020. As more and more IoT devices are connected and communicated, IoT applications generate tremendous IoT traffic. Since IoT traffic is for the communication between objects, the transmission reliability is critical, especially in a relatively unstable WSN, compared with wired network. As Figure 1 shows, IoT technology is applied in many domains, including environmental monitoring, transportation, automotive vehicles, industry, medical technology, healthcare, smart home, and smart city.

Fig. 1 IoT application domains [3].


Smart home and city
Internet of Things reliably connects everything
E-health
Mobile and transportation
Everyday things
Industry 4.0

A routing protocol decides how to send packets to other nodes. Routing protocols have two major divisions including Reactive and Proactive routing protocols. Routes are providing by the reactive protocols when it is needed. When it is necessary, control messages are transmitted by the path of data transfer, using these types of protocols. But, the needed time to find the route is increases. In addition, control messages are periodically exchanged by the proactive routing protocols immediately after start in order to search and propagate the routes. Local control messages together with messages across the entire network are sent by nodes to receive local nearby information and to share the structural information in all nodes of the network. A categorizing of router protocols is illustrated in Figure 2.

Fig. 2 Categorizing of router protocols [4].



In this research, we propose Multi-path routing protocol (GSTMPR-IoT). The developed GSTMPR-IoT protocol includes three key sections: a novel approach of distributed cluster discovery which can automatically establish local nodes, an innovative set of algorithms to adjust clusters and their head alternations based on the centralized position and isotropic energy propagation in all the sensing nodes, and a brilliant mechanism to reduce energy loss in long distance telecommunication.

The paper presented here is organized as the following. Section 2 introduces some relevant terms regarding multi-path routing. In Sect. 3 brings the proposed GSTMPR-IoT schema. Moreover, parameters utilised for performance evaluation are investigated and simulation results are discussed in Section 4. Finally, in Section 5, the paper is concluded.

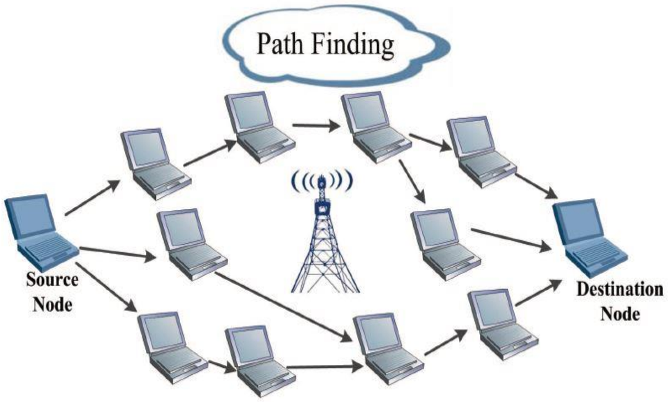
2 Relevant terms

This section provides an introduction to the central concepts of this paper: multi-path routing, and detection schemes to provide protection for the IoT.

2.1 Multi-path routing

A new IoT technique called multi-path routing is capable of solving instability difficulties, narrow bandwidth, and energy protection. By use of this technique, the effect of network connection failures is decreased. It has a significant effect on performance improvement of IoT network. However, multipath calculations are more complicated job than single path calculations. It is difficult because of finding optimal multiple paths. By this method, it is possible to compute multiple paths in an independent and distributed manner. It is established based on multi-path disjunction principle that between the same source–destination pair, the disjunction may be partial or not. The aim of disjunction principle is to guarantee the paths independency; it means connection failure one of the paths will not affect the other ones. For transmitting a data packet between a source and a destination, it is possible to use any path of a multipath. Therefore, to get the most out of the data flow, and maximize share of the network bandwidth, the streams of data packets between a source and a destination can be divided between the paths. Figure 3 illustrates multipath routing in IoT [5].

Fig. 3 Multipath routing in IoT.



2.2 Detection schemes

In recent years, there have been many suggested researches on real-time routing protocols. And the central focus of them is divided into two main problems about multi-path routing protocols. The first one is the protocol requirement to guarantee the reliability of real-time packets in order to decrease the number of blank regions created by loss and delay. The other one is the protocol requirement to stabilize the energy loss of the network and avoid early expiration of some nodes.

SMH-GEAR Method: In the work done by Zhang et al. in 2017, while taking into consideration the characteristics of the internet of things, multiple energy routing and hybrid routing algorithm are presented. An efficient model with high organization for nodes in large scale according to GEAR protocol is proposed. The proposed GEAR protocol, is based on the SMH model. This model consists of the following: discovering the route of fixed nodes, discovering the route of moving nodes, routing maintenance and routing processing. This model is based on the following assumptions:

- There is a sync node in the network.

- The nodes are sorted in a two-dimensional topology.
- Node positions, remaining energy and movement speeds are known.
- Initial state of the network is such that the sync node has infinite energy and other nodes have constant energy.

This model is a hybrid multi-routing model based on the little world model named hybrid multi-routing model based on the little world model (SMH). In this paper, the model is run and an improved model based on GEAR is obtained which is the SMH-GEAR protocol. Then the SMH-GEAR and GEAR protocols are compared. The simulations are carried out using NS-2 simulation tool. The results are compared and analysed with respect to four aspects: success rate in packet aggregation, end to end latency, network performance and network lifetime. Simulation results indicate that this protocol can increase network lifetime and achieve optimization in network throughput and network globalization. Overall, experimental results represent that the performance of the SMH-GEAR protocol is better than the GEAR protocol [6].

Energy Transfer Algorithm Based on RPL: RPL is an IPV6 network and is created similar to a tree topology. It is based on criteria optimization process in a small network using different objective functions (OF) for carrying out the intended routing process. In the paper, Mahmud et al. proposed a routing protocol and energy transfer algorithm for designing a system based on RPL with reliable energy and low cost for IoT applications in 2017. The information of DODAG is needed to route the traffic in RPL network. It is specified in DODAG which node is the parent. RPL protocol collects the information available in DODAG. DODAG uses control packets named DODAG Information Object (DIO) and information request (DIS) collects the information available in DODAG. The objective of this paper is achieving efficient energy in the system for IoT applications in such a way that by using less energy, the nodes guarantee the lifetime of the network. Furthermore, this algorithm improves the throughput of the network. Simulation results indicate that each node can select an optimal energy level for transmission. Although the simulations are carried out for two nodes, the proposed system can work for a larger number of nodes. Limitation of our proposed model is that all the considered items are homogeneous where the nodes have the RF CC2420 transmitter. The proposed method might not work properly on a network with heterogeneous nodes and other TF receivers [7].

SCOTRES Method: George Hatzivasilis et al. developed a method named SCOTRES in 2017 for secure routing based on important criteria such as energy in internet of things network. SCOTRES is a trust based system for secure routing in ad-hoc networks which use smart devices to transmit information. The proposed method is described using five criteria. Energy criterion, takes into consideration the resource consumption of each node. Trust criterion increases the network lifetime. Topology criterion is aware of the node positions and enhances loading. Chanel health criterion, due to inappropriate channel conditions, protects the network against harmful attacks. Reputation criterion evaluates each of the participants of specific network operations for identification of specialized attacks. On the other hand, trust criterion, general adaptation, evaluates the fulfilment against hybrid attacks. Performance and effectiveness of the proposed method was evaluated in NS-2 simulator and SCOTRES is merged with DSR routing protocol. Similar patterns are carried out using the same platform in order to have a fair comparison. SCOTRES has two types: one is embedded systems, and the other is real systems. The evaluations represented in this paper demonstrated that this system has the highest protection rate, while maintaining the performance for setting up real applications [8].

ERGID Method: A routing protocol called Emergency Response IoT based on Global Information Decision (ERGID) was suggested in the study of Qui et al. in 2016 to increase the reliability of data transmission performance and efficiency of the emergence response to IoT. Especially, in this study a mechanism called delay iterative method (DIM) which is founded on delay approximation was designed to answer the problem of disregarding valid routes. Additionally, a transfer plan called "Remaining Energy Probability Choice" (REPC) was recommended for balancing the network load together with focusing on the remained energy of the node. Consequences and examination of the simulation indicates that ERGID have better performance with respect to EA-SPEED and SPEED approaches regarding end to end delay, packet dissipation rate, and energy loss. Also, in this study some applied examinations were performed using STM32W108 sensing nodes. It was detected that ERGID can increase the network ability for real-time response [9].

AOMDV Technique by means of SDN: In a research published by Kharkongo et al. in 2016, an AOMDV based routing protocol was suggested in which the power loss of heterogeneous devices has considered. Furthermore, An SDN controller is offered in the network which archives in an integrated style and creates a secure network by performing as an administrator that rejects access to selfish nodes in the network. The hypothesis of this study includes:

- The SDN controller is registered with devices
- There are different energy amounts for Heterogeneous devices
- The overall network traffic is monitored by a centralized controller

The stages of the suggested algorithm are listed below:

- Stage 1: The controller is registered with the nodes. The controller allocates an exclusive ID to every node in the network.
- Stage 2: The network is monitored by the controller.
- Stage 3: The source node discovers the information affecting the neighbour node.
- Stage 4: Remained energy of the neighbourhood node is calculated.
- Stage 5: Based on the node energy, the source node transmits the packet. If the energy value is under the threshold value, the packet is sent. Else, other neighbour node is chosen.
- Stage 6: The controller will stop the selfish node by preventing it to add the network again.

This study compares the AOMDV routing with SDN controller to other AODV routing protocols, DSR and DSDV. Achieved results with altered parameters determine that the suggested routing protocol has better performance than traditional routing protocols regarding to efficiency, packet delivery rate, and average end to end delay. Consequently, total performance of the network enhances using the suggested routing method [4].

AOMDV-IOT Technique: In this study, the suggested technique called AOMDV-IOT is introduced. It is a routing technique and up to the destination, it can perform as the router. The recommended method is not offered just for the node. The enhancements are mostly appropriate in IoT which is a unique technique for it. The principle object in this technique is detecting and generating effective connections between the nodes and the internet using the AOMDV routing protocol in the IoT. The internet connection table (ICT) is added in the suggested routing protocol to every node. Every node has two tables in this method including: routing table and ICT. ICT consists of four units: terminal node number, terminal node IP address, lifecycle, and hop value. Even though ICT uses extra memory, instead it can store connection counts and consequently decreases transmission delay. Comparison of AOMDV, simulating outcomes show that AOMDV-IOT has improved efficiency with respect to end to end delay, packet loss, and frequency in IoT. In this research, the multi-objective ad-hoc generated distance vector for the internet of things has been enhanced in such an approach that it can dynamically choose the direct internet transmission route by regular update of internet link table. Simulating effects show that while the AOMDV-IOT routing protocol rises the two routing packets, average end to end delay of the route falls [10].

EECRP Method: In the next paper, Shen et al. in 2017 proposed a new and centralized energy-based routing protocol (EECRP) for the internet of things with the help of wireless sensor networks to improve the network performance. They presumed that wireless sensor nodes are randomly distributed in the network. It has also been assumed that each node knows the BS location and the remaining energy value all the time. In the method proposed in this paper:

- A clustering algorithm that acts according to the location of energy base and remaining energy of the nodes.
- An optimization algorithm which is added to the protocol according to the number of dead nodes and cluster heads.
- In order to decrease long distance communications, a protection mechanism has been described for EECRP to save energy in cluster heads.

The proposed EECRP protocol consists of three key sections: a new distributed cluster detection method which is able to automatically organize local nodes, a new set of algorithms to adapt clusters and cluster head rotations based on the centralized location and uniform energy distribution among all of the sensor nodes, and a new mechanism for reducing long distance communication energy consumption. Node energy calculation has been considered in EECRP in order to calculate the centralized location. Simulation results show that EECRP performs better that LEACH, LEACH-C, and GEEC. Furthermore, EECRP is suited for networks that require a long lifetime and have a base station (BS) node. When the BS is in the network, EECRP can send a significant amount of data with very low energy loss. Therefore, network lifetime is longer for EECRP than it is for LEACH [11].

AOMDV method: A self-correcting path detection and information transferring route is suggested by AlZubi et al. for enabled applications in the Internet of Things (IoT). This routing procedure achieves at device level for self- restore and establishing its communication routes in a large-scale network. The routing practice is naturally opportunistic, need local device information instead of universal update. This opportunistic routing (OR) is built on best-fit traversing (BFT) algorithm to enhance the device availability in a precise way. The best-fit algorithm determines perfect neighbours for restarting interrupted communications in elongated mode [12].

Adaptive Distributed Routing Method: FANET networks are a key part of the IoT and can offer messaging facilities for various devices in the IoT and cyber-permitted applications. But, moving unmanned aerial vehicles (UAV) in FANETs creates random network link and increases complexity of routing algorithms for these applications, particularly in real-time routing. In this research, an effective opportunistic distributed routing technique is suggested to explain the above mentioned problem. For data transfer in this process, only the colleague nodes and local information are used by the transmitter. They maximize network use and preserve the end to end delay less than a stated threshold in order to care for variations of network and channel by designing and solving an optimization problem. Besides, they guess one stage delay for every communication of the transmitter node and use double parsing to alter the integrated problem into a distributed one. By this method, the transmitter nodes are only permitted to contact with local information and approximate delay in packet routs. Simulation outcomes indicate that the introduced routing technique enhances the network performance regarding its energy efficiency, quantity, and end to end delay [13].

REL Method: In the next work, Machado et al. proposed an energy and link quality-based routing protocol (REL) for IoT applications. In order to improve reliability and energy efficiency, REF selects an estimator mechanism based on the end to end link and the remaining energy. Furthermore, REL proposes an event-based mechanism to maintain load balance and prevent premature energy loss in nodes and the network. REF provides an end to end route selection plan based on cross-layer information with minimum overhead. In order to achieve energy efficiency, the nodes send their remaining energy to the neighbouring nodes. In this paper, route selection process is carried out using end to end link quality evaluation and optimal energy information. A new method is used for link quality estimation. REL utilizes the wireless link quality and the remaining energy while routing in order to increase system reliability and support QoS for IoT applications. REL uses a reactive pattern for discovering routes. This results in reduced signalling overhead and improved scaling capability. Route discovery process consists of diffusing RREQ and RREP messages. Performance evaluation was carried out using simulation and experimentation to demonstrate the effects and advantages of REL in small and large networks. Simulation experiments for evaluating REL and comparing it to AODV and LABILE protocols with respect to energy efficiency, latency and packet delivery are carried out in large scenarios and for various internet of things applications. In large scale networks with high node density, results suggest that in REL, lifetime was improved up to %26.6, latency up to %17.9, and packet delivery up to %12 when compared to AODV and LABILE. The results show that REL improves the network lifetime, service availability, and also the quality of internet of things applications. It also makes it possible to redistribute rare network resources and decreases packet loss with respect to well-known protocols [14].

MLB Method: Internet of things is based on wireless sensor networks (WSN) and ZigBee is one of the most popular wireless sensor network protocols. In the internet of things, large data transfers using wireless sensor networks has caused many problems. However, AODV routing stack in ZigBee protocol has no load balancing mechanism to handle corrupted traffic. Therefore, we develop multi-path load balancing (MLB) to replace AODV routing protocol in ZigBee. MLB is proposed for collaboration with ZigBee wireless network in the large scale. In this scenario, ZigBee is used as communication media in wireless sensor networks. In order to create a reliable ZigBee stack, ZigBee network layer is placed in MLB. MLB provides alternative routing service for ZigBee network without altering the existing stack in ZigBee. When a ZigBee router transmits the IoT data forward, MLB guides the ZigBee network layer in selecting the next hop with minimum load towards the IoT gate.

MLB consists of two main schemes: layer design and load balance. Layer design assigns the nodes to different layers based on their distance to the IoT gate. Nodes can present multi-dimensional IoT data. All of the neighbouring nodes in the layer transfer information in the form of load flow and are used for load balancing and load estimation in later steps. Using MLB, the nodes can select neighbours with the least load in later steps and therefore load balance can be achieved and bottlenecks be avoided. Comparing AODV ZigBee with its multi-path counterpart, the AOMDV protocol, demonstrates that MLB has better load balance, lower packet loss, and higher routing connection rate in both of the network and random topologies. MLB provides a reliable method for routing and internet of things applications [3].

NLEE Algorithm: In the paper presented by Vellanki et al. in 2016, the effective energy protocol for improving energy efficiency in internet of things was introduced. The proposed algorithm, makes decisions that minimize upload using shortest paths. This method uses the expected remaining node energy countdown and total number of node transfers as the routing criteria to improve energy efficiency. This method controls the number of transferred and broadcasted packets to discover routes. Furthermore, route discovery is carried out using remaining energies and step counts of the nodes in the routes. Moreover, NLEE algorithm guarantees better utilization of the energy available in the nodes. It also regularizes routing delay while discovering the shortest path in the network [15].

Table 1, summarizes the investigated efforts to design multi-path routing for IoT.

Table 1 Concludes the examined ways to design multi-path routing for IoT.

References	Operation	Advantages	Disadvantages
SMH-GEAR [6]	Taking into consideration the energy criterion for multi-path routing	Increased network lifetime and throughput	Not taking into account other important network criteria
RPL-Based System [7]	Takin into consideration the energy criterion for routing	Attaining an energy efficient method in the internet of things by improving network lifetime	This method might not work properly with some types of RF receivers. Also other important network criteria have not been considered
SCOTRES [8]	Secure routing with emphasis on energy consumption of the devices and decreasing it	Increased network lifetime while using trust criterion in order to prevent hybrid attacks	-
ERGID [9]	Routing based on decisions made with general information	Improved data transfer performance and emergency response	The need to estimate delay in order to improve delay and network lifetime
[4]	Routing in the internet of things based on the AOMDV protocol	Detecting malicious nodes in the network and packet transfer based on the energy and improved network efficiency	Not taking into account other criteria such as distance etc. along the way of the packet
AOMDV-IoT [10]	Discovering and establishing efficient link between nodes and the internet based on the AOMDV protocol	Decreased latency and decreased packet loss rate	More overhead because of storing two tables in each node and two extra routing packets
EECRP [11]	Clustering algorithm while taking into account the energy criterion while routing and selecting the cluster heads	Distributed clustering and uniform load distribution among all of the sensor nodes	Not taking into account criteria other than energy while routing
Adaptive Distributed Routing Method [13]	Reducing the complexity of routing algorithms using distributed adaptive routing	Improved energy efficiency, throughput, and end to end latency	The need to carry out exact calculations to calculate delay
REL [14]	Routing protocol based on link quality and energy	Improved reliability and energy efficiency	-
MLB [3]	Layer design and balancing load in order to create load balance and eliminate bottlenecks	Load balancing, decreased packet loss, and increased connections	Paying no attention to the remaining energy and lifetime of the node
NLEE [15]	Efficient energy protocol for improving energy efficiency in the internet of things	Improved latency – decreased power consumption	Overhead caused by counting the number of sent and control packets, step count and remaining energy

3 The proposed GSTMPR-IoT schema

In the following section, we design a GSTMPR-IoT schema by employing the Gray System Theory algorithm. The proposed system consists of six steps, such as the overview of the GSTMPR-IoT schema is discussed in Sect, 3.1. Adding new parameters to AOMDV is discussed in Sect, 3.2. Designing the routing packets in GSTMPR-IoT is discussed in Sect. 3.3, Gray System Theory Steps is discussed in Sect. 3.4, Using gray theory in routing is discussed in Sect. 3.5, and the algorithm for the proposed GSTMPR-IoT method is discussed in Sect. 3.6.

3.1 Overview of the GSTMPR-IoT schema

In this paper, in order to eliminate the disadvantages of previous methods, gray system theory, which is a multi-criterion decision making method, is used for selecting appropriate routes. In this study, several criteria such as remaining energy in the node, link expiration time, hop count, and signal to noise ratio are used for routing. In this scheme, AOMDV routing protocol is used. AOMDV routing protocol is the multi-path version of the AODV routing algorithm. This protocol tries to discover separate link routes with separate nodes. All of the routing tables in AOMDV include a list of multiple routes for each destination to support multi-path routing. All of the routes pertaining to a destination have an identical sequence number. In order to ensure that the routes in the routing table are link-separate, each node removes the route request messages that have the same next hop or the same last hop to one of the existing routes in the routing table. While all of the nodes follow this rule, all of the routes with the same sequence number will have separate links. In this section, this protocol is improved so that it can discover appropriate short and high energy routes. The proposed method named Gray System Theory based Multi-Path Routing for the Internet of Things (GSTMPR-IoT) is presented.

In this section, first the way new parameters are added to the AOMDV is described. Then, each one of the service parameters used in this paper are explained briefly. Finally, usage of the gray system theory is described comprehensively.

3.2 Adding new parameters to AOMDV

Because most of the devices are wireless, link stability fluctuation caused by movement or transfer medium characteristics in the internet of things affects the network performance. Efficiency of a dynamic routing protocol can be rated based on its ability to handle link unreliability and its computational and reconfiguration/rerouting overhead. Link stability as the basis of routing can lead to a protocol that has the following capabilities:

Efficient Energy: Fewer disconnected links because of reduced rerouting, resulting in low connection and computational overhead.

Movement Flexibility: Selected links are durable for longer periods of time against lost connections in moving nodes.

Stability: In order to reduce the overhead of the routing tables, more effective routes are stored longer. We evaluate the link stability in our work with the energy, step count, signal to noise ratio, and route expiration time parameters corresponding to each route.

Signal to noise ratio is presented as $SINR$. The higher the $SINR$ value is, the higher are the chances of continuous connection and link for longer periods of time. The higher the remaining energy in a node, the higher are its chances of staying alive for longer periods of time and therefore the larger its transmission range. The higher the link expiration time (LET) and the lower the number of hops, the higher are the chances of the packets being delivered quickly and soundly.

Signal to Noise Ratio: Noise ratio is defined as the ratio of the received signal (S) to a combination of noise strength (N) and interference (I). Definition of $SINR$ is presented in Equation (1):

$$SINR = \left(\frac{S}{N+I} \right) \quad (1)$$

$SINR$ is estimated using the average reception during inactivity period. $SINR$ is used to determine the quality of network links or connections.

Remaining Energy (Re): One of the most important elements while choosing a route is the remaining energy in the nodes along that route. The higher the remaining energy in the nodes of a route and the lower their consumed energy, the more appropriate that route is to be selected. Remaining energy is calculated using Equation (2).

$$ER_N = \left(EP_N(t) - ECo_N(t) \right) \quad (2)$$

In Eq. (2):

$ER_N(t)$: *Remaining energy of the node*

$EP_N(t)$: *Primary energy of the node*

$ECo_N(t)$ *Consumed energy of the node*

Hop Count (Hop): The Hop count parameter is the number of Hops between the origin node and the destination node. The lower the Hop count of a route, the better that route is because less energy needs to be used in order to transmit the packet.

Link Expiration Time (LET): It is the amount of time for which the links stays stable. The longer this time period is, the more stable the link between the nodes will be. This parameter depends on the movement speed of the nodes. The faster the nodes move, the more unstable the route between them will be and the sooner it will be destroyed. Link expiration time is calculated using Equation (3) based on the transmitted packets between the nodes.

$$LET(i, j) = \frac{-(ab+cd) + \sqrt{(a^2+c^2)*R^2 - (ad-bc)^2}}{a^2+c^2} \quad (3)$$

$$a = v_i * \cos\theta_i - v_j * \cos\theta_j,$$

$$b = x_i - x_j,$$

$$d = Y_i - Y_j,$$

$$C = v_i * \sin\theta_i - v_j * \sin\theta_j$$

The nodes are aware of their location using GPS. In the above equation there are two nodes i and j which are at (x_i, y_i) and (x_j, y_j) respectively. Their speeds are v_i, v_j and their movement angles are θ_i and θ_j. In the following section, details for each step are presented.

3.3 Designing the routing packets in GSTMPR-IoT

In the proposed method, all of the devices need to be equipped with GPS and have maximum initial energy. AOMDV routing packet format is expanded so that it can be used for GSTMPR-IoT routing. This is achieved by adding new fields to AOMDV routing packets. GSTMPR-IoT routing protocol, just like the base AOMDV protocol, has four packet formats. However, in the proposed GSTMPR-IoT method, these formats are altered and required fields are added to these packets. Details of these packets are presented below.

HELLO Packet: This packet is used to discover neighboring devices in regular intervals. Adjacent nodes exchange their location obtained through GPS and remaining energy information using HELLO packets. After exchanging the HELLO packet, each node updates its routing table and the remaining energy of neighboring nodes and also calculates $SINR$ rate based on the received signal from the neighbor and link expiration time (LET) with the neighboring node based on its own location and the neighbor's location and also writes them into its table.

Fig. 4 New format of the HELLO packet.

<table>
<tr><td>Packet type</td><td colspan="2">Reserved</td><td>Unused</td></tr>
<tr><td colspan="2">Origin IP address</td><td colspan="2">Origin sequence number</td></tr>
<tr><td colspan="2">Time stamp (origin time)</td><td colspan="2">Node energy</td></tr>
<tr><td colspan="2">Node location</td><td colspan="2">Node speed</td></tr>
</table>

RREQ Packet: The second packet is the route request ($RREQ$) packet. Each time a node tries to communicate with other nodes in the network, route discovery process needs to be carried out. Therefore, the node broadcasts the $RREQ$ packet publicly to find an appropriate route to its destination $RREQ$ packets consist of an ID to identify each packet, the destination IP address, sequence number, and network time stamp. Destination sequence number indicates the freshness of a route. We add the remaining node energy, $SINR$ value, and the calculated LET with the last hop based on the $HELLO$ message fields to the $RREQ$ packet. Each node has calculated these parameters based on the Eq. (1) through Eq. (3) upon receiving the $HELLO$ message and saved them in its table. Now, once the $RREQ$ message is received, each node on this route adds these information and transfers to the next node along the route to the destination.

Fig. 5 New format of the *RREQ* packet.

<table>
<tr><td>Packet type</td><td colspan="2">Reserved</td><td>Hop count</td></tr>
<tr><td colspan="2">RREQ public broadcast ID</td><td colspan="2">Destination IP address</td></tr>
<tr><td colspan="2">Destination sequence number</td><td colspan="2">Origin IP address</td></tr>
<tr><td colspan="2">hop count</td><td colspan="2">Node remaining energy</td></tr>
<tr><td colspan="2">Time stamp</td><td colspan="2">Accumulated route</td></tr>
<tr><td colspan="2">SINR</td><td colspan="2">LET</td></tr>
</table>

RREP Packet: The third packet is the route reply packet. After receiving the broadcasted $RREQ$ packets, many routes are discovered from the origin to the destination. Normally, $RREP$ packet consists of an ID to identify unique packets, origin IP address, sequence number, and accumulated routes. In the proposed method, we get the destination of every $RREQ$ packet from different routes and calculate the total number of hops, total remaining energy in each route, and total $SINR$ and LET in the links of each route and add them to the $RREP$ packet. Then, this packet is sent to the origin of that route. Therefore, we add the new total remaining energy of the route nodes, hop count, and total $SINR$ and LET fields to the $RREP$ packet.

Fig. 6 New format of the *RREP* packet.

<table>
<tr><td>Packet type</td><td colspan="2">Reserved</td><td>Hop count</td></tr>
<tr><td colspan="2">ID RREP</td><td colspan="2">Destination IP address</td></tr>
<tr><td colspan="2">Origin sequence number</td><td colspan="2">Origin IP address</td></tr>
<tr><td colspan="2">Accumulated route</td><td colspan="2">Time stamp</td></tr>
<tr><td colspan="2">Total remaining energy of the nodes along the route</td><td colspan="2">Total hop count along the route</td></tr>
<tr><td colspan="2">Total SINR along the route</td><td colspan="2">Total LET along the route</td></tr>
</table>

RERR Packet: Whenever a node discovers an error, it broadcasts a route error ($RERR$) packet with the destination sequence number and infinite hop count. The origin node or any other node along the route can rebuild the route by sending a $RREQ$ packet. If the origin node or any other node receives the $RRER$ packet, it needs to re-execute the route discovery process.

3.4 Gray System Theory Steps

When units are evaluated using different parameters, some important parameters might be neglected. This happens specially when performance parameters have several values. Also, if the objectives and instructions of these parameters are different, results of analyzing them will be misleading. Therefore, performance evaluation parameters must be converted to a comparable sequence and therefore normalization is required. This is the gray relation creating step.

In order to evaluate several devices, if m is the number of devices and n is the number of parameters, then the device number i will be described as $Y_i = \left(y_{i1}, y_{i2}, ..., y_{ij}, ..., y_{in}\right)$ where Y_i is the value of parameter j for device i.

Y_i can be converted to a comparable sequence $X_i = \left(x_{i1}, x_{i2}, ..., x_{ij}, ..., x_{in}\right)$ using Equation (4) and Equation (5). In other words, these parameters can be normalized using the presented equations.

$$X_{ij} = \frac{y_{ij} - Min\left\{y_{ij}, i = 1, 2, ..., m\right\}}{Max\left\{y_{ij}, i = 1, 2, ..., m\right\} - Min\left\{y_{ij}, i = 1, 2, ..., m\right\}} \quad (4)$$

$$X_{ij} = \frac{Max\left\{y_{ij}, i = 1, 2, ..., m\right\} - y_{ij}}{Max\left\{y_{ij}, i = 1, 2, ..., m\right\} - Min\left\{y_{ij}, i = 1, 2, ..., m\right\}} \quad (5)$$

In Equation (4) and Equation (5), i and j are defined as follows:

$$i \in \left\{1, 2, 3, ..., n\right\}, j \in \left\{1, 2, 3, ..., m\right\} \quad (6)$$

Equation (4) is used for positive parameters. In this equation, the bigger X_{ij} is, the better the obtained results will be. In the proposed scheme, this equation is used for the remaining energy, link expiration time, and noise rate parameters. Equation (5) is used for negative parameters. In this equation, the smaller X_{ij} is, the better the results will be. This equation is used for the HOP count parameter. After creating the gray relations using the above equations, all of the performance values, just like normalized values, will be between zero and one. The closer X_{ij} is to one, the parameter will be more desirable. Therefore, the comparative series consisting of all ones will be the best choice. The target series is a series where all of the performance values are equal to one. Equation (7) illustrates the target series (X_0) where all of its parameters are equal to one.

$$X_0 = \left(x_{i1}, x_{i2}, ..., x_{ji}, ..., x_{in}\right) = (1, 1, ..., 1, ..., 1) \quad (7)$$

After this step, the main goal is finding a unit which is as close to this target series as possible. In order to find such a unit, gray coefficients must be calculated first. Steps to calculating this parameter are presented in the following section.

3.4.1 Gray Relation Coefficient

In the next step, gray relation value needs to be measured. This value is the gray relation rank. Calculating the gray relation rank requires the gray relation coefficient to be calculated first. Gray relation coefficient is used to determine the proximity of X_{ji} with X_{0j}. Equation (8) is used to calculate the gray coefficient.

$$\gamma\left(x_{0j}, x_{ij}\right) = \frac{\Delta_{\min} + \varepsilon\Delta_{\max}}{\Delta_{ij} + \varepsilon\Delta_{\max}} \tag{8}$$

In this equation, $\gamma\left(x_{0j}, x_{ij}\right)$ is the gray coefficient and its value is between x_{ji} and x_{oj}. In Equation (8), values of Δ_{ij}, $\Delta_{\min}$, and $\Delta_{\max}$ are defined as Equation (9).

$$\begin{aligned} \Delta_{\min} &= Min\left\{\Delta_{ij}, i = 1,2,\ldots,m;\ j = 1,2,\ldots,n\right\} \\ \Delta_{\max} &= Max\left\{\Delta_{ij}, i = 1,2,\ldots,m;\ j = 1,2,\ldots,n\right\} \end{aligned} \tag{9}$$

In these equations, Δ_{ij} is used to measure the difference between x_{ij} and x_{oj}, while $\Delta_{\min}$ is the minimum value among all of the parameters and $\Delta_{\max}$ is the maximum value among all of the parameters.

ε in Equation (8) is the detection coefficient which is a number in the $[0,\ 1]$ interval. In most of the studies, ε is set to 0.5. After calculating the gray relation coefficient, gray relation rank is calculated for the aforementioned items. In the following section, how to calculate this rank is presented.

3.4.2 Calculating the Gray Rank

Gray coefficient of two parameters is between zero and one in such a way that if this coefficient is one, it means that those two parameters are equivalent. On the other hand, if the coefficient is zero, those two parameters are independent. After calculating the gray coefficient, gray rank can be calculated using Equation (10) and use the resulting value in making various decisions.

$$T\left(X_0, X_i\right) = \sum W_j * y\left(x_{0j}, x_{ij}\right) \tag{10}$$

In this equation, $T\left(X_0, X_i\right)$ represents the gray relation between X_0 and X_i which demonstrates the correlation between the reference sequence and the compared sequence. W_j is the weight or importance coefficient which is a parameter determined according to the problem structure. In our method, due to its higher importance, we have set the weight for the energy parameter higher than other parameters in the simulations. Equation (11) always holds for all the W_j

$$\sum_{j=1}^{n} W_j = 1 \tag{11}$$

In other words, according to the above equation, summation of all the weight values will be equal to one. Gray rank presents the similarity between the compared sequence and the reference sequence. The reference sequence for each evaluated unit represents the best possible performance which can be achieved using the compared sequence. This way, after the rank of every route has been determined according to their remaining energy, hop count, noise rate, and link expiration time parameters, the best route to the destination which has the best devices will be selected. This sequence is repeated until the decision-making process is completed. Because the final values are unities numbers between zero and one, overall rank of the route can be calculated according to the average gray rank of the mentioned parameters.

3.5 Using Gray Theory in Routing

As mentioned in the previous sections, in this this research the quality of service, remaining energy level, noise rate ($SINR$), link expiration time, and hop count parameters are used to select the best route for efficient diffusion of information in the internet of things. Studies show that information diffusion using an efficient algorithm can significantly improve the performance of the internet of things. In this paper, several routes get selected for multi-path diffusion of information by checking the quality of service parameters of the devices (nodes). In other words, quality of service parameters of each node is used to select the best route for information diffusion. In related works, one or two quality of service parameters were used for information diffusion in the internet of things. The advantage of the proposed method is that it combines different quality of service parameters to determine the appropriate routes to diffuse information through. Using several parameters to solve in deterministic optimization problems can lead to optimal or near-optimal solutions. However, it should be noted that using too many parameters can significantly increase the computational complexity and therefore decrease the network performance. The proposed GSTMPR-IoT routing method for the internet of things consists of three steps. Neighbor discovery step, route discovery step, and data transfer step. We will describe each step in the following sections.

3.5.1 Neighbor Discovery Step

In the neighbor discovery step, nodes (devices) flood the network with *HELLO* packets to find their neighbors. The *HELLO* packet includes the origin IP address, remaining energy of the node, node location, node speed, sequence number, and time stamp. After the neighbor discovery step, every device knows all of its neighbors in the network and is aware of their location and remaining energy. The nodes also calculate the *SINR* value for their immediate neighbors using the received signal and the noise rate and interference values. Also, using the location and speed of the neighboring node in the last step and their own location and speed, each node calculates the link expiration time (*LET*) of its link with the neighboring node. Each node stores this information for its immediate neighbors.

3.5.2 Route Discovery Step

When the origin node decides to send a packet to the destination, it floods the network with *RREQ* packets to discover the suitable routes. *RREQ* packet includes the IP address of the origin and destination, sequence number, hop count, remaining energy in the node, *LET* , *SINR* , accumulated route, and time stamp. IP address of the origin and the destination are used to identify unique nodes in the network. The destination sequence number is used to show the suitable routes to the destination. Each node after receiving the *RREQ* packet, retrieves its neighbor information and inserts it into its routing table. Then inserts the new information along with its own information into the *RREQ* packet and sends it to the next node. Figure 7 demonstrates the flooding of *RREQ* packets in the network in order to find routes leading to the destination. Figure 8 demonstrates the *RREP* packets sent by the destination node to the origin node.

Fig. 7 Flooding RREQ packets.

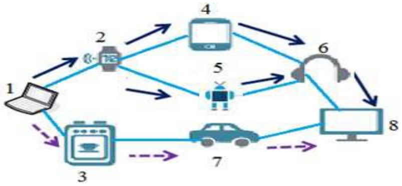
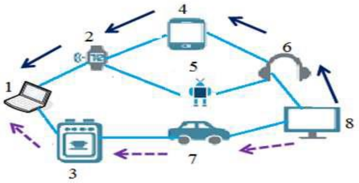


Fig. 8 Transmission of the RREP packet.



The destination node received multiple *RREQ* packets using different routes. Also, the *RREP* packet includes the node ID to identify unique packets, destination IP address, sequence number, lifespan in the network, and accumulated routes. The accumulated routes are a list of separate routes from origin to destination. Moreover, three new fields, namely the total *LET* of each route, total *SINR* , and remaining energy of each route calculated by the destination node using the *RREQ* packets are added to the *RREP* packet. After adding these fields, the destination node sends the *RREP* packet using all of the routes and stores this information in its routing table. The origin node, upon receiving the *RREP* packets from destination, stores the origin of these multiple routes in its routing table.

3.5.3 Data Transmission Step

After discovering several routes, the origin node calculates the total value of each parameter for all of the routes and saves them in a table. Table 2 is used to demonstrate the quality of service parameters for the nodes.

Table 2 Parameters of Quality of Service for each of the routes.

Parameters/Routes	Total hop Count	Total Time to Expiration of the Link Between the Nodes	Total Remaining Energy	Total SINR
1	$\sum hop_1$	$\sum LET_1$	$\sum ERn_1$	$\sum SINR_1$
2	$\sum hop_2$	$\sum LET_2$	$\sum ERn_2$	$\sum SINR_2$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
n	$\sum hop_n$	$\sum LET_n$	$\sum ERn_n$	$\sum SINR_n$

Now with the total value of the quality of service parameters for each of the routes to the destination known, gray relation theory is used to solve the problem. Since the abovementioned parameters have different units and therefore cannot be compared directly, a normalization method needs to be used to normalize the values and make them comparable. The normalization methods used in the gray theory are presented in Equation (4) and Equation (5). These equations have several applications. Equation (4) is used to normalize positive parameters while Equation (5) is used for normalization of negative parameters. In this research, three of the parameters are positive parameters which include the remaining energy, noise rate, and link expiration time. However, the hop count parameter is a negative one. In other words, the lower this parameter is, the better and therefore more desirable the final result will be. Therefore, Equation (4) is used to normalize the three positive parameters while Equation (5) is used to normalize the negative parameter. The values yielded after normalization using Equation (4) and Equation (5) for all of the parameters of the routes will be a scalar between zero and one. Value equal to one is the optimal condition and zero is the worst case. Therefore, one is considered as the reference series. As mentioned before, the reference series is presented as $X_0 = \left(x_{i1}, x_{i2}, \ldots, x_{ji}, \ldots, x_{in}\right) = (1,1,\ldots,1,\ldots,1)$ where all of the normalized parameters are equal to one. After the most similar series to the reference series is determined for all of the nodes, the main goal is finding a route which is as close to the reference series as possible. Gray coefficient is used to find such a route. How to calculate the gray coefficient is presented in Equation (8). After determining the gray coefficient for all of the routes and their parameters, gray rank is used for ranking all of the routes based on the aforementioned quality of service parameters. How to calculate the gray rank using the parameters for the routes is presented in Equation (10) and Equation (11). The values resulted from this equation is a 1×n column matrix where n is the total number of available routes to the destination. This matrix consists of a decreasingly suitable sequence routes (based on the quality of service parameters) for information diffusion. The routes for multi-path routing of data are selected from the indices of the matrix with the highest gray rank values. These routes are saved in the table. This is repeated until the destination is changed or the route is eliminated.

Selecting the routes with better quality of service parameters, i.e. with high link expiration time, high signal to noise ratio, and high energy levels and low hop count to the destination, while reducing the network latency, improves its performance. After each cycle of data diffusion in the network, values for each of the mentioned parameters are updated for every node and the above steps are repeated for the next information diffusion round. The data transmission and routing process used in the proposed GSTMPR-IoT method is presented in figures 9 and 10.

3.6 The Algorithm for the Proposed GSTMPR-IoT Method

The overall steps of the algorithm for the proposed method based on the gray system theory for multi-path diffusion of information in the internet of things networks is as presented in figure 9. The proposed algorithm is repeated for each round of information diffusion after updating the quality of service parameters.

Fig. 9 Pseudo code of the proposed GSTMPR-IoT method.

Algorithm (4): Pseudo code for GSTMPR-IoT proposed schema

```
1:  Routing initialization by the sender node.
2:  The sender node checks its routing table to see whether a route to the destination exists?
3:      If there is no route to the destination, sending the RREQ and RREP packets for
4:          discovering routes between the sender and the destination is carried out. Then go to step 6.
5:      If there are route from the sender to destination, go to step 6.
6:  Calculate sum of the parameters for each of the available routes to destination.
7:  Normalize the quality of service parameters using the gray theory normalization method.
8:  Determine parameter series for each route.
9:  Calculate the gray coefficient for each of the series created in step 8.
10: Calculate the gray rank for all of the routes.
11: Select the routes with highest gray rank for simultaneous diffusion of information packets.
12: Send the packets using the chosen routes.
13: Check the acknowledgements to see if the packets were received in the specified time period.
14:         Acknowledgement packet was received, go to step 16.
15:         Acknowledgement packet was not received, return to step 3.
16: Repeat the above steps after updating the quality of service parameters.
17:End
```

In the proposed GSTMPR-IoT method, the traffic is distributed uniformly among the selected routes. This method guarantees that the energy of the nodes along the routes are used uniformly because the sender node will always select the routes with highest gray rank to ensure route reliability with regard to energy, link expiration time, and also noise rate. In other words, the probability of the links being broken is reduced and therefore it is used more often than other routes. The proposed method also prevents the nodes from dying prematurely and the network being destroyed.

The flowchart for the proposed GSTMPR-IoT method is presented in figure 10. All of the steps to the proposed algorithm, from start to finish, can be found in this flowchart.

doi:10.20944/preprints202001.0304.v1

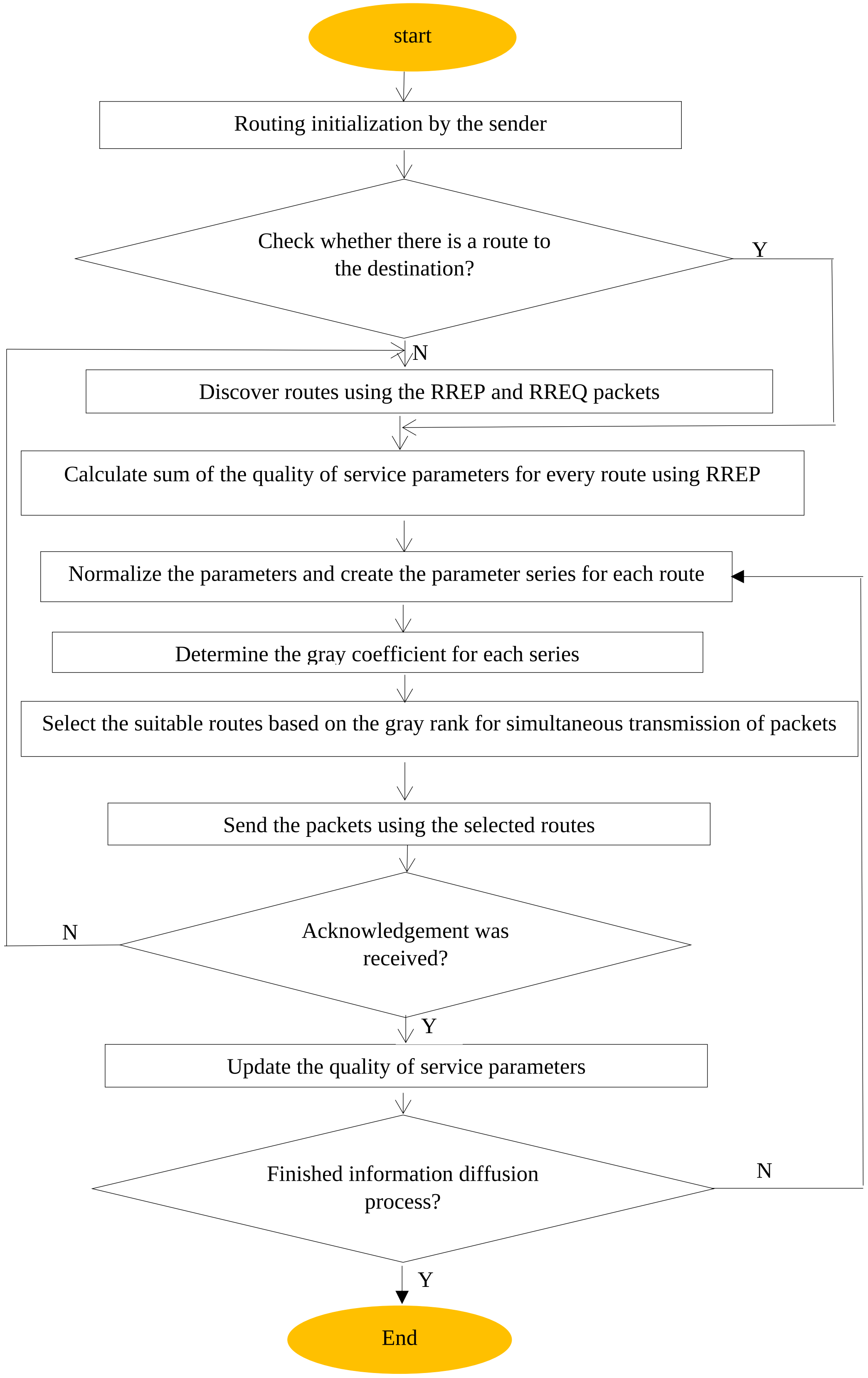

start
Routing initialization by the sender
Check whether there is a route to the destination?
Y
N
Discover routes using the RREP and RREQ packets
Calculate sum of the quality of service parameters for every route using RREP
Normalize the parameters and create the parameter series for each route
Determine the gray coefficient for each series
Select the suitable routes based on the gray rank for simultaneous transmission of packets
Send the packets using the selected routes
N
Acknowledgement was received?
Y
Update the quality of service parameters
Finished information diffusion process?
N
Y
End

Fig. 10 Flowchart of the GSTMPR-IoT.

4 Evaluating the Performance

In the following section, the performance of our proposed GSTMPR-IoT approach is evaluated to multi-path routing problem.

5.1 Performance metrics

In this section, the effectiveness and performance of our proposed GSTMPR-IoT approach is thoroughly evaluated with comprehensive simulations. The results are compared with EECRP and AOMDV approaches proposed in [11] and [12], respectively. The throughput, packet delivery rate, end to end delay, average residual energy, and network lifetime are evaluated. Notations utilised here are listed in Table 3.

Table 3 Abbreviated notations

Parameters	Description
$AT\_$	Average throughput
PDR	Packet delivery rate
$E2E$	End-to-End delay
NL	Network lifetime
ARE	Average Residual Energy
N	Number of Things
X_i	Demonstrate the Number of packets received by thing I
Y_i	Demonstrate the Number of packets sent by thing I

5.1.1 *Average Throughput*

Average throughput is the division of the sum of packets sizes received at the destination sensor node, to the difference of simulation stop and start time [16]. Eq. (12) obtains the average throughput for N experiments, and is calculated in Kilobits per second.

$$AT\_ = \frac{1}{n} * \frac{\sum_{i=1}^{n} X_i * P_s}{S_p - S_T} * \frac{8}{1000} \tag{12}$$

5.1.2 *Packet delivery rate*

PDR is the division of the total data packets received at the destination thing, to the total number of data packets transmitted by the source thing, described in percentage [17]. The average PDR obtained for N experiments is demonstrated by Eq. (13).

$$PDR = \frac{1}{n} * \frac{\sum_{i=1}^{n} X_i}{\sum_{i=1}^{n} Y_i} * 100\% \tag{13}$$

5.1.3 *End to End Delay*

It is defined as the average latency between the transmitting of packets by the source and its reception by the receiver. This contains all probable latencies produced in data acquisition, route detection, queuing, middle nodes processing, resending delays at the MAC, broadcast time, etc. Its measuring unit is milliseconds. The lesser amount of end-to-end latency means the better efficiency of the protocol [18]. Equation (14) shows calculated end-to-end latency as follows:

$$E2E = \left(\frac{\sum_{j=1}^{n} Delivery\ Time - \sum_{j=1}^{n} Arrival\ Time}{\sum_{i=1}^{n} Recieved\ packets} \right) \tag{14}$$

5.1.4 *Average Residual Energy*

As demonstrated in Eq. (15), unconsumed energy in the node in an arbitrary time instance is the excessive energy maintained in the node following a concluded communication with the receiver. Examples of residual energies are the energy for transmission, energy for reception, wasted energy in the system (E_{sys}), fading effects, etc. The parameters exploited for the average residual energy are listed in Table 4.

Table 4 Parameters used for average residual energy

Parameters	Description
di_0	Reference distance larger than the Fraunhofer-distance
di	The distance on which the packet is transmitted
Lb	demonstrates the number of bits per packet (BPP)
di^2	Refers to the power loss of free space channel model
di^4	Power loss of multi-path fading channel model
E_{elec}	Amount of energy getting dissipated during transmission or reception
$lb \in fsi$	Transmission efficiency
$lb \in mpi$	Condition of the channel

$$Energy_{residual} = Energy_{initial} - \left\{ ET_X + ER_X + E_{sys} \right\} \quad \text{Where} \tag{15}$$

$$ET_X(1b, di) = \left\{ lbE_{elec} + lb\varepsilon_{fs} di^2, di < di_0 \right\} \tag{16}$$

$$= \left\{ lbE_{elec} + lb\varepsilon_{mpi} di^4, di \geq di_0 \right\}$$

Energy consumed during packet transmission $ET_X(1b, di)$ and packet reception (ER_X) are calculated using Eq. (16), and Eq. (17), respectively.

$$ER_X = lbE_{elec}. \tag{17}$$

Simulated parameter is set as: $\left\{ \begin{array}{l} E_{elec} = 100nJ / bit, \\ \varepsilon_{fsi} = 20 pJ / bit / m^2, \\ \varepsilon_{mpi} = 0.0015 pJ / bit / m^4 \end{array} \right\}$

If $di > di_0$, multipath fading effect occurs, and energy is wasted during transmission. However, since the fading scheme is out of the scope of this paper, the distance is considered to be lesser than the Fraunhofers distance. Moreover, the information for channel state is not considered, while transmission efficiency is considered to be 1.

5.1.5 *Network Lifetime*

According to the definition, the network lifetime is the elapsed time between of communication and sensing commencement with the receiver, and the time in which the final communication link from active node to the receiver is broken. Network lifetime for all active nodes currently in communication with the receiver is the life time aggregate for all the mentioned nodes at any time instance. If the network is clustered, the network lifetime is the total lifetime for all things [19]. Eq. (18) demonstrated the calculation of the NL value.

$$NL = \sum_{i=1}^{m} Things_i \qquad \text{Where} \qquad Things_i \text{ is the lifetime of } i \text{ th things.} \tag{18}$$

5.2 Simulation setup and comparing algorithms

The difficulties in implementation and debugging IoTs in real networks, raises the necessity to consider simulations as a fundamental design tool. The main advantage of simulation is simplifying analysis and protocol verification, mainly in large-scale systems. In this section, the performance of our proposed approach is evaluated using NS-3 as the simulation tool, and the results are discussed further. It is worth mentioning that all GSTMPR-IoT, EECRP and AOMDV parameters and settings are considered to be equal.

5.3 Simulation results and Analysis

In this section, we analyze the performance of GSTMPR-IoT under the two scenarios (described in Table 5). There are 500 IoT things uniformly deployed in the network area initially. Some important parameters are listed in Table 5.

Table 5 Setting of simulation parameters.

Parameters	Value
Coverage area (m x m)	First scenario: 2000 x 2000 Second scenario: 4000 x 4000
Simulation tool	NS-3
MAC layer protocol	IEEE 802.11
Transport	UDP/IPv6
Communication range of each node	300 m
Channel bandwidth	3 Mbps
Traffic type, rate	CBR, 10 packets/sec
Mobility model	Random way point
RX and TX ratio	90%
Number of nodes, and Packet size	500, 256 Kbps
Number of connections, and Pause time	50, 100 sec
Maximum mobility (varying)	5 m/sec - 25 m/sec
Simulation time (in Sec)	500-2000

Table 6-10 compares the performance of GSTMPR-IoT with that of EECRP and AOMDV in terms of throughput, packet delivery rate, end to end delay, average residual energy, and network lifetime.

Table 6 $AT\_$ (in Kbps) of various frameworks with varying degree of rate of transmission (kb/s).

Rate of Transmission (kb/s)	Average throughput (Kbps)		
	$AOMDV$	EECRP	$GSTMPR-IoT$
5	710	1100	1540
15	830	1307	1700
25	1208	1580	2105
35	1480	1770	2540
45	1704	1890	2800
55	1903	2100	3100
65	2080	2470	3430

Table 7 *PDR* (in %) of various frameworks with varying degree of rate of transmission (kb/s).

Rate of Transmission (kb/s)	PDR (%)		
	AOMDV	EECRP	*GSTMPR – IoT*
5	58.23	67.4	83.4
15	6013	70.1	86.4
25	64.2	72.9	89.6
35	65.4	76.3	90.1
45	68.3	77.4	92.4
55	71.1	79.3	95.3
65	73.9	81.7	97.4

Table 8 *E2E Delay* (in m/sec) of various frameworks with varying degree of rate of transmission (kb/s).

Rate of Transmission (kb/s)	E2E Delay (m/sec)		
	AOMDV	*EECRP*	GSTMPR-IoT
5	804	704	430
15	930	734	445
25	947	780	460
35	1100	839	490
45	1203	840	520
55	1440	920	540
65	1600	970	586

Table 9 *ARE* (in Joule) of various frameworks with varying degree of rate of transmission (kb/s).

Rate of Transmission (kb/s)	ARE (Joule)		
	AOMDV	*EECRP*	GSTMPR-IoT
5	820	950	1104
15	810	912	1040
25	740	900	940
35	701	850	910
45	680	843	904
55	632	831	890
65	591	790	870

Table 10 *NL* (in Sec) of various frameworks with varying degree of rate of transmission (kb/s).

Rate of Transmission (kb/s)	NL (Sec)		
	AOMDV	*EECRP*	GSTMPR-IoT
5	590	780	1000
15	501	710	890
25	435	650	830
35	406	595	797
45	395	515	760
55	350	430	715
65	320	418	704

Table 11 represents average values of various frameworks for all metrics.

Table 11 Average values of various frameworks for all metrics.

Schemes		*AT _*	*PDR*	*E2EDelay*	*ARE*	*NL*
AOMDV	Number of Things	693.1	66.659	1867.7	522.8	764.7
	Simulation times	817.9	68.84	1461.4	673.5	369.8
	Mobility speed	1104.5	53.8	1124.3	498	258.1
	Number of Things	905	75.418	1618.2	691.3	857
	Simulation times	1034.6	80.599	1080	737.2	428.6

EECRP	Mobility speed	1288.3	70.298	864.6	673	273.5
GSTMPR-IoT	Number of Things	1588.2	96.29	759.3	841.1	1111.1
	Simulation times	1751	97.243	664.1	900.9	818.5
	Mobility speed	2008.8	88.61	512.9	831	636.9

Average throughput: Figure 11 shows the comparison of the GSTMPR-IoT proposed scheme, EECRP and AOMDV models in term of $AT\_$. (a) Number of Things, (b) Simulation times, and (c) Mobility speed respectively. As shown in the diagrams, the proposed method outperforms the EECRP and AOMDV methods with regard to throughput as well. This was to be expected due to the superior packet delivery rate and also low delay. In the proposed GSTMPR-IoT method, routes with high energy levels, fewer hops to the destination, long expiration time, and low noise rate are selected for data transmission. Taking into account all of these criteria and selecting the routes according to gray theory has led to high throughput in the proposed method.

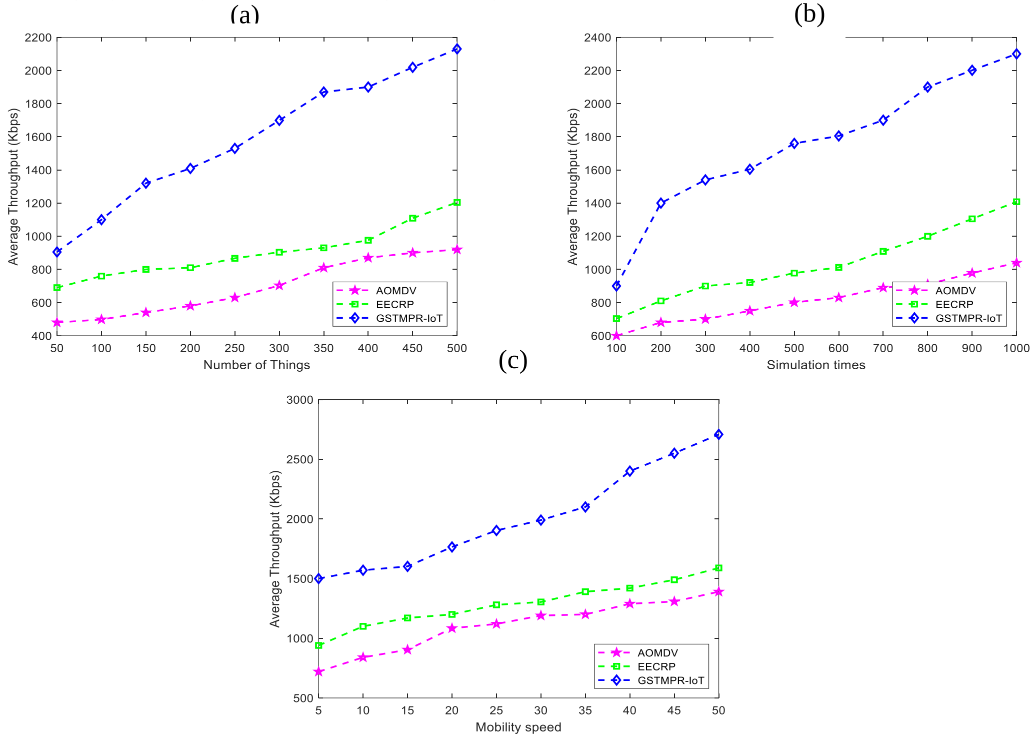


Fig. 11 Comparison of the GSTMPR-IoT proposed scheme, EECRP and AOMDV approaches in term of Throughput. (a) Number of Things, (b) Simulation time, and (c) Mobility speed.

Figure 12 shows the relationship PDR and (a) Number of Things, (b) Simulation times, and (c) Mobility speed respectively under the same setting as Table. 5. As seen in figure 12, the proposed method in this paper (GSTMPR-IoT) has better packet delivery rate than EECRP and AOMDV. This is because in the proposed method, packet routing is done through the routes with high remaining energy and expiration time. Also, the nodes along these routes transmit the packets with more power. In the GSTMPR-IoT, data packets are transmitted through several routes selected according to the gray theory with higher rank compared to other routes. Also, taking into account the hop count and link expiration time parameters along with the important remaining energy criterion ensures that the route is not destroyed and energy of the nodes is not depleted while packets are being transmitted which leads to more packets being delivered to their destination.

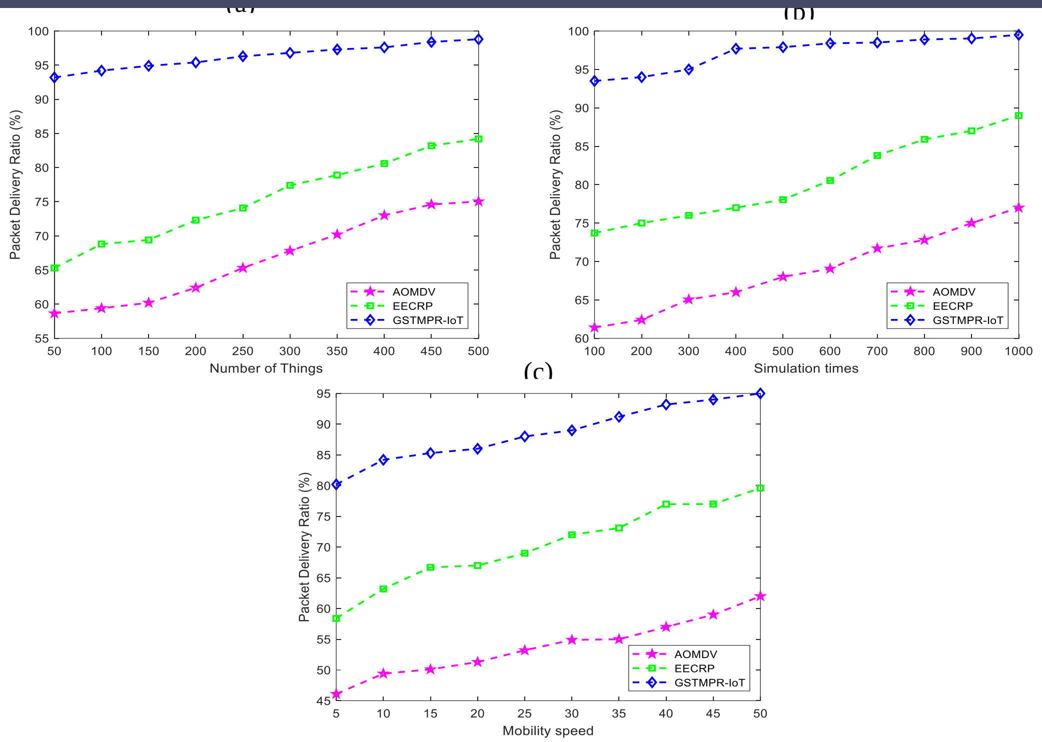


Fig. 12 Comparison of the GSTMPR-IoT proposed scheme, EECRP and AOMDV approaches in term of PDR. (a) Number of Things, (b) Simulation time, and (c) Mobility speed.

Figure 13, shows E2E delay against (a) Number of Things, (b) Simulation times, and (c) Mobility speed respectively. The proposed GSTMPR-IoT method in this paper has lower E2E delay compare to the EECRP and AOMDV methods. The main reason for this is that in the proposed method, the packets are transmitted in a multi-path fashion and the packets are sent using the best selected routes simultaneously while in the EECRP method, each packet is sent using the cluster head. Also, in the proposed method the hop count parameter has also been taken into account which leads to the shortest routes to the destination being selected. This way, the data is delivered to the destination with lower delay.

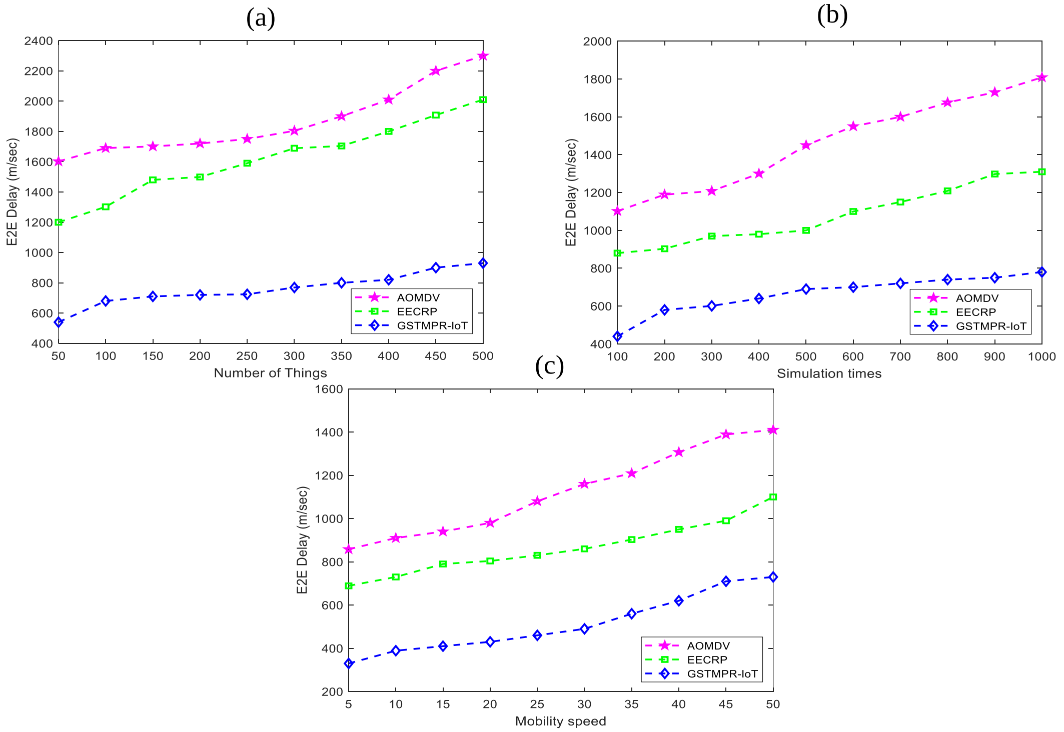


Fig. 13 Comparison of the GSTMPR-IoT proposed scheme, EECRP and AOMDV approaches in term of End to End Delay. (a) Number of Things, (b) Simulation time, and (c) Mobility speed.

Figure 14 shows the comparison of the GSTMPR-IoT proposed scheme, EECRP and AOMDV models in term of *ARE* . (a) Number of Things, (b) Simulation times, and (c) Mobility speed respectively. Due to limited resources such as power, energy, bandwidth, processing power, and storage capacity of the nodes and also to reduce the routing overhead and ensure high packet delivery rate, the remaining energy in the network is an important matter in the internet of things networks. This criterion presents the *ARE* in the nodes after routing has been carried out and is calculated using equation 13 which is calculated by subtracting the consumed energy from the initial energy. As seen in figure 14, the *ARE* in the nodes is calculated at 100 and 1000 seconds in every simulation. The simulation results present that the *ARE* in the nodes for the proposed GSTMPR-IoT is higher than the EECRP and AOMDV methods. This is because in the proposed method, routing is carried out using routes which consist of nodes which are better than the nodes in other routes with respect to hop count, noise rate, *ARE* , and link expiration time criteria. Therefore, taking into account the hop count criterion leads to lower energy consumption, while selecting the route which consists of nodes with higher energy levels controls the network energy and increases the *ARE* . Therefore, the proposed method performs better in this regard as well. Repeating this process at each information diffusion step leads to the routes with the best nodes being selected and therefore, compared to EECRP and AOMDV, the energy consumption is increased distributes across the network. As can be seen in the presented diagrams, the proposed GSTMPR-IoT method performs much better compared to the EECRP and AOMDV methods with regard to the remaining energy and fluctuates less. Stability of the nodes in the network leads to a better network where nodes are not prone to premature deactivation due to excessive energy consumption. In the proposed GSTMPR-IoT method, while the energy depletes as time goes by, but this decrease in energy levels is much lower than the EECRP method and the proposed method has higher energy levels compared to EECRP and AOMDV at any given time. The energy depletion is inevitable but because out method constantly selects the routes with higher energy levels for information diffusion, more energy is conserved in the nodes compared to the EECRP and AOMDV method.

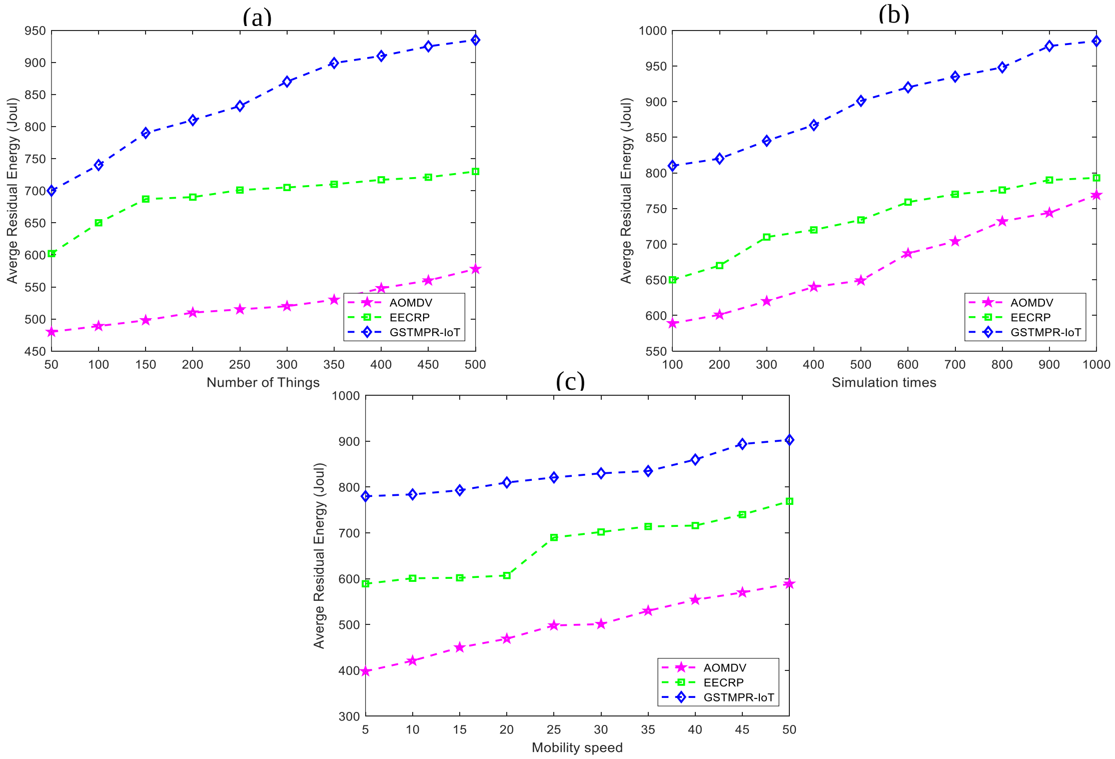


Fig. 14 Comparison of the GSTMPR-IoT proposed scheme, EECRP and AOMDV approaches in term of Average residual energy. (a) Number of Things, (b) Simulation time, and (c) Mobility speed.

Network lifetime is the time period while the network is stable and is able to transmit data packets. Network lifetime is calculated using equation 12. The remaining energy in the mobile nodes affects network lifetime directly. As presented in figure 15, the proposed GSTMPR-IoT method outperforms the EECRP and AOMDV methods when it comes to network lifetime as well. In the GSTMPR-IoT method, by choosing high energy routes with fewer hops, premature deactivation of nodes in the network is prevented. Since the routes are selected for data transmission based on their remaining energy and fewer hops while also taking into consideration their noise rate and link expiration time, energy in the network nodes is depleted over a longer period of time and network lifetime is increase. In the simulations as time goes by, network lifetime decreases. However, network lifetime is longer when compared to the EECRP and AOMDV methods. The reduced lifetime as time goes by is due to energy consumption and deactivation of the nodes.

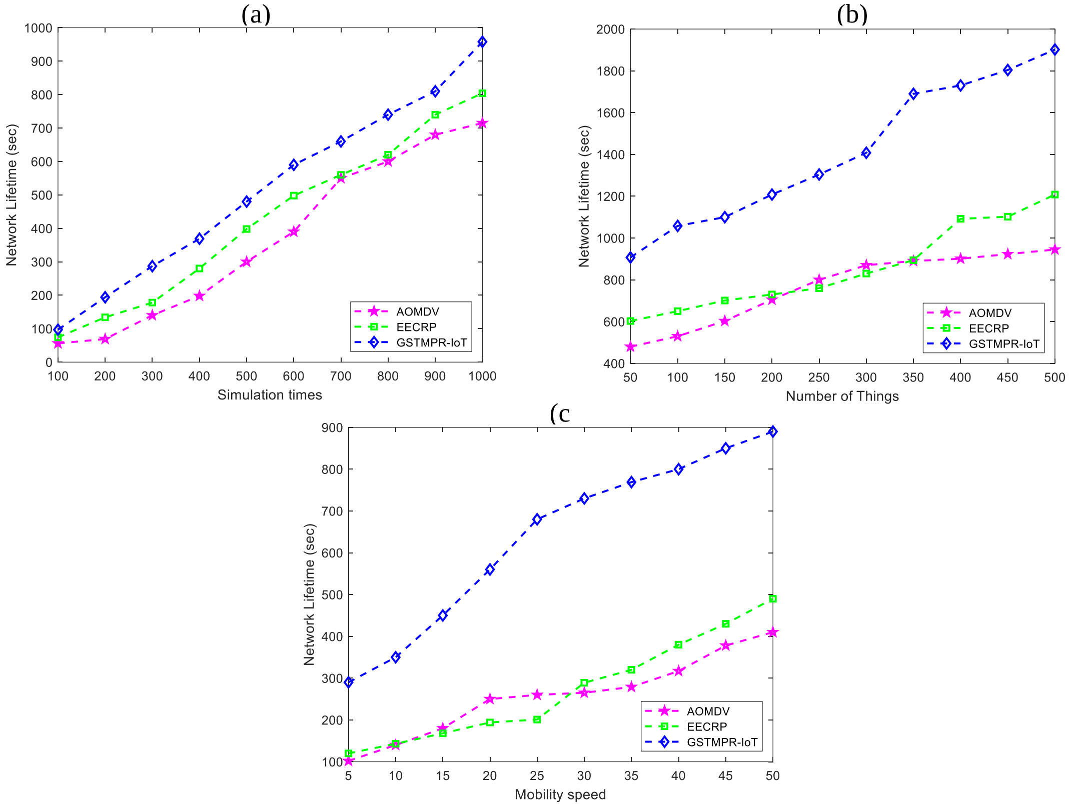


Fig. 15 Comparison of the GSTMPR-IoT proposed scheme, EECRP and AOMDV approaches in term of Lifetime. (a) Number of Things, (b) Simulation time, and (c) Mobility speed.

6 Conclusion

Internet of things is a heterogeneous network that includes the traditional internet and the network of limited devices which are connected through the IP protocol. The devices in the internet of things are unique and identifiable devices that sense and test the connection between the physical environment or host devices and the internet. In reality the devices in IoT are highly heterogeneous and many of them have limited resources and therefore their global connectivity creates an important challenge for the internet of things. Therefore, this network faces multiple challenges regarding energy consumption and reliable connectivity and the inherent features of these networks, such as dynamic topology and energy constraints, has made the routing problem very challenging. In order to tackle this issue, researchers are constantly searching for new and effective methods to solve the problems present in these networks. AOMDV routing protocol is the multi-path version of the AODV protocol. This protocol tries to discover routes with separate links and nodes to send data through. Since multiple routes to the destination are used, in this paper this method has been chosen for routing in the internet of things meaning that AOMDV has been improved by utilizing important criteria such as energy, link expiration time, and signal to noise ratio. Also, gray system theory is used to select the best and optimal routes. In order to create this method, we use the hop count, mid-route nodes energy, link expiration time, and signal to noise ratio parameters for routing in GSTMPR-IoT. To use these criteria, AOMDV standard packet format was changed and new fields were added to it. Afterwards, using the gray system theory to rank the routes, best routes were selected to transfer data through. We have analyzed the performance of our GSTMPR-IoT scheme using NS-3, and showed that it exhibits a high-level of performance with a high throughput (more than 93.12%)%), and high PDR (more than 93.01%), and low E2E delay (less than 24.65%), and high average residual energy (less than 26.32%), and high network lifetime (more than 89.16%), as compared to current approaches.

Reference

1. Liu, A., et al., *A green and reliable communication modeling for industrial internet of things.* Computers & Electrical Engineering, 2017. 58: p. 364-381.
2. Qiu, T., R. Qiao, and D.O. Wu, *EABS: An event-aware backpressure scheduling scheme for emergency Internet of Things.* IEEE Transactions on Mobile Computing, 2018. **17**(1): p. 72-84.
3. Tseng, C.H., *Multipath load balancing routing for Internet of things.* Journal of Sensors, 2016. 2016.
4. Seyedi, B., & Fotohi, R. NIASHPT: a novel intelligent agent-based strategy using hello packet table (HPT) function for trust Internet of Things. The Journal of Supercomputing, 1-24.
5. Fotohi, R., et al., *An Improvement over AODV routing protocol by limiting visited hop count.* International Journal of Information Technology and Computer Science (IJITCS), 2013. **5**(9): p. 87-93.
6. Jamali, S. and R. Fotohi, *DAWA: Defending against wormhole attack in MANETs by using fuzzy logic and artificial immune system.* the Journal of Supercomputing, 2017. **73**(12): p. 5173-5196.
7. Jamali, S. and R. Fotohi, *Defending against wormhole attack in MANET using an artificial immune system.* New Review of Information Networking, 2016. **21**(2): p. 79-100.
8. Jamali, S., Fotohi, R., Analoui, M. (2018). An Artificial Immune System based Method for Defense against Wormhole Attack in Mobile Adhoc Networks. TABRIZ JOURNAL OF ELECTRICAL ENGINEERING, 47(4), 1407-1419.
9. Kharkongor, C., T. Chithralekha, and R. Varghese, *A SDN Controller with Energy Efficient Routing in the Internet of Things (IoT).* Procedia Computer Science, 2016. 89: p. 218-227.
10. Hasan, M.Z. and F. Al-Turjman, *Optimizing multipath routing with guaranteed fault tolerance in Internet of Things.* IEEE Sensors Journal, 2017. **17**(19): p. 6463-6473.
11. ZHANG, X.-j., Z.-y. QU, and M.-l. ZHANG, *A High Efficient Self-Organizing Network Protocol for Large Scale Aware Nodes in Internet of Things.* DEStech Transactions on Engineering and Technology Research, 2017(amma).
12. Fotohi, R., & Jamali, S. (2014). A comprehensive study on defence against wormhole attack methods in mobile Ad hoc networks. International journal of Computer Science & Network Solutions, 2, 37-56.
13. Fotohi, R. (2020). Securing of Unmanned Aerial Systems (UAS) against security threats using human immune system. Reliability Engineering & System Safety, 193, 106675.
14. Fotohi, R.; Nazemi, E. An Agent-Based Self-Protective Method to Secure Communication between UAVs in Unmanned Aerial Vehicle Networks. Preprints 2020, 2020010229 (doi: 10.20944/preprints202001.0229.v1).
15. Mabodi, K., Yusefi, M., Zandiyan, S., Irankhah, L., & Fotohi, R. Multi-level trust-based intelligence schema for securing of internet of things (IoT) against security threats using cryptographic authentication. The Journal of Supercomputing, 1-25.
16. Zandiyan S, Fotohi R, Koravand M. P-method: Improving AODV routing protocol for against network layer attacks in mobile Ad-Hoc networks. International Journal of Computer Science and Information Security. 2016 Jun 1;14(6):95.

17. Fotohi, R., Heydari, R., & Jamali, S. (2016). A Hybrid routing method for mobile ad-hoc networks. Journal of Advances in Computer Research, 7(3), 93-103.
18. Fotohi, R., & Bari, S. F. (2020). A novel countermeasure technique to protect WSN against denial-of sleep attacks using firefly and Hopfield neural network (HNN) algorithms. The Journal of Supercomputing, 1-27.
19. Fotohi, R., Bari, S. F., & Yusefi, M. (2019). Securing Wireless Sensor Networks Against Denial-of-Sleep Attacks Using RSA Cryptography Algorithm and Interlock Protocol. International Journal of Communication Systems.
20. Fotohi, R., Ebazadeh, Y., & Geshlag, M. S. (2016). A new approach for improvement security against DoS attacks in vehicular ad-hoc network. International Journal of Advanced Computer Science and Applications, 7(7), 10-16.
21. Behzad, S., Fotohi, R., Balov, J. H., & Rabipour, M. J. (2018). An Artificial Immune Based Approach for Detection and Isolation Misbehavior Attacks in Wireless Networks. JCP, 13(6), 705-720.
22. Behzad, S., Fotohi, R., & Jamali, S. (2013). Improvement over the OLSR routing protocol in mobile Ad Hoc networks by eliminating the unnecessary loops. International Journal of Information Technology and Computer Science (IJITCS), 5(6), 2013.
23. Behzad, S., Fotohi, R., & Dadgar, F. (2015). Defense against the attacks of the black hole, gray hole and wormhole in MANETs based on RTT and PFT. International Journal of Computer Science and Network Solutions (IJCSNS), 3, 89-103.
24. Sarkohaki, F., R. Fotohi, and V. Ashrafian, *An efficient routing protocol in mobile ad-hoc networks by using artificial immune system.* International Journal of Advanced Computer Science and Applications (IJACSA), 8 (4), 2017.
25. Mahmud, M.A., A. Abdelgawad, and K. Yelamarthi. *Energy efficient routing for Internet of Things (IoT) applications*. in *2017 IEEE International Conference on Electro Information Technology (EIT)*. 2017. IEEE.
26. Hatzivasilis, G., I. Papaefstathiou, and C. Manifavas, *SCOTRES: secure routing for IoT and CPS.* IEEE Internet of Things Journal, 2017. 4(6): p. 2129-2141.
27. Qiu, T., et al., *ERGID: An efficient routing protocol for emergency response Internet of Things.* Journal of Network and Computer Applications, 2016. 72: p. 104-112.
28. Tian, Y. and R. Hou. *An improved AOMDV routing protocol for internet of things*. in *2010 International Conference on Computational Intelligence and Software Engineering*. 2010. IEEE.
29. Shen, J., et al., *An efficient centroid-based routing protocol for energy management in WSN-assisted IoT.* IEEE Access, 2017. 5: p. 18469-18479.
30. AlZubi, A.A., M. Al-Ma'aitah, and A. Alarifi, *A BEST-FIT ROUTING ALGORITHM FOR NON-REDUNDANT COMMUNICATION IN LARGE-SCALE IoT BASED NETWORK.* Computer Networks, 2019.
31. Wen, S., et al., *Energy-efficient and delay-aware distributed routing with cooperative transmission for Internet of Things.* Journal of Parallel and Distributed Computing, 2018. 118: p. 46-56.
32. Machado, K., et al., *A routing protocol based on energy and link quality for internet of things applications.* sensors, 2013. 13(2): p. 1942-1964.
33. Vellanki, M., S. Kandukuri, and A. Razaque, *Node level energy efficiency protocol for Internet of Things.* Journal of Theoretical and Computational Science, 2016. 3.