International Journal of Scientific Research in Computer Science and Engineering
Vol.10, Issue.6, pp.49-60, December (2022)
Review Paper
E-ISSN: 2320-7639

Routing In Mobile Ad-Hoc Networks Coupled With IoT Technologies- A Review

GATETE Marcel[1*], HARUBWIRA Flaubert[2]

[1,2]Dept. Business Information Technology, University of Tourism, Technology, and Business Studies-UTB, Kigali, Rwanda

[*]*Corresponding Author: mgatete@utb.ac.rw, Tel.: +250784003392*

Available online at: www.isroset.org

Received: 20/Sept/2022, Accepted: 22/Nov/2022, Online: 31/Dec/2022

Abstract— A self-organizing, decentralized, and dynamic network known as MANET allows nodes to join and exit at any time and from any location. Routing in MANET is challenging because a node may quit the network while a packet is traveling the path it must take to reach its destination. This is because each node in this form of wireless network can simultaneously serve as a host and a router. There are benefits and drawbacks to nodes' capacity to organize themselves, which is a crucial component of MANETs. This facilitates network upkeep and topology change, but data transfer must be tolerated. Although the MANET is utilized for both big networks and the internet, there aren't always smart IoT-enabled devices that can transfer data between locally and remotely linked PCs. More individuals now use the Internet to access information and technology from around the world. In order to establish worldwide business prospects that can benefit from the I-GVC (Information-driven Global Value Chain) for enhanced productivity, the Internet of Things is largely utilized to connect applications and services. The Internet of Things (IoT) is a relatively new field that makes use of a variety of sensors, devices, controllers, processes, and services to link the real and virtual worlds. Many different physical items can be employed to aid in human work. In light of this, the Internet of Things is a cutting-edge technology that offers a practical method for bridging the physical and digital worlds via a variety of networks and communication methods. Smart surroundings where it interacts with MANET make it more user-friendly and profitable. New MANET-IoT systems and IT-based networks can be created thanks to how mobile ad hoc networks and the Internet of Things interact. The cost of deploying the network is decreased while user mobility is increased. In terms of networking, it also brings up some fresh, difficult problems. This study compares the three types of IoT-enabled Mobile Ad Hoc Networks (MANETs) protocols, Proactive, Reactive, and Hybrid, and discusses their applicability to be best fit for the realization of the IoT environment, notably for routing. We first go into great detail on each form of IoT-enabled ad hoc network protocol, their architecture, and features. Then, we compare protocols in each category. Finally, we undertake an overall comparison of all three types of protocols in MANET specifically for IoT.

Keywords— Internet of Things, MANET, Mobile Nodes, Network Evaluation Metrics, Routing Protocols, Rev

I. INTRODUCTION

1.1 Mobile Ad Hoc Network

1.1.1 Introduction

MANET, also known as a wireless Adhoc network or Adhoc wireless network, is an acronym for mobile ad hoc network. It is often built on top of a link layer ad hoc network and features a routable networking environment. They consist of a group of mobile nodes that are wirelessly linked together in a self-configuring, self-healing network that lacks a fixed infrastructure. MANET nodes can move around at whim because the network topology is always changing.

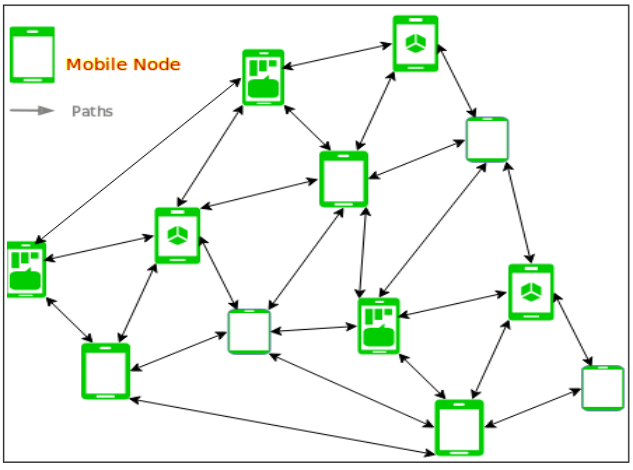

Figure 1: MANET Structure

The MANET's key difficulty is providing each device with the data it needs to appropriately route traffic. MANETs

are peer-to-peer, self-forming, self-healing networks that typically operate between the years 2000 and 2015. They interact over radio frequencies (30MHz-5GHz).

Road safety can benefit from using sensors for the environment, the house, health, disaster relief operations, air/land/navy defense, weaponry, robotics, and other applications [2].

1.1.2 Inherent Features of MANETs

1. Multi-hop Routing1: Data packets should be routed through one or more intermediary nodes when travelling between wireless networks. Because wireless transceivers' signal propagation characteristics make multi-hop communications necessary [8], MANETs must be able to provide multi-hop routing for mobile nodes that can't reach the destination node when the message's source and destination nodes are out of radio range. A message from the source to the destination node must pass through several nodes because of the constrained transmission radius. Each node serves as a router and forwards packets from other nodes to enable multi-hop routing [9].

2. Dynamic Network Topology: Data packets should be passed via one or more intermediary nodes when being sent from a source to a destination over a wireless network. as a result of the signal Any node in a MANET is free to relocate or join at any time without knowing its neighbors, but the network is able to autonomously manage its topology. MANET nodes can enter and exit the network at any time, changing its linkages and topology because they are mobile. Additionally, bidirectional or unidirectional connections between nodes are possible. But because of this function, there are a lot of users and they move around a lot.

3. Infrastructure-less Nature: Independent peer-to-peer nodes work together to create MANETs by communicating with one another for a specified goal [7]. All devices function equally within the network and there is no previous base station or organization. There are also no pre-defined roles like routers or gateways because the network's nodes are provided; instead, each device can serve as both a node and a router simultaneously. Its actions are independent, and nodal connectivity is sporadic.

4. Bandwidth Constraints and Variable Link Capacity: Compared to cable connections, connections between MANET nodes have substantially less bandwidth[7]. Multiple accesses have a variety of negative impacts, including multipath fading, noise, congestion, fluctuation, and signal interference.

5. Limited Resources (Light-Weight Terminals): Small hand-held devices including laptops, smartphones, personal digital assistants (PDA), and mobile phones make up the majority of MANET hardware. These devices only have a little amount of storage space and battery power.

6. Fluctuating Link Capacity: In a MANET, the The nature of wireless connections' high bit-error rates could be more serious. Several sessions may share the same end-to-end path. The communication channel between the terminals has a less bandwidth than a wired network and is susceptible to noise, fading, and interference. Occasionally, the route between any two users may involve a number of wireless links, each of which may be heterogeneous.

8. Inadequate Physical Security: Wireless connections made MANET vulnerable to physical layer intruders including eavesdroppers, jammers, spoofers, and DDoS attacks (DoS). However, MANETs are better protected against single failure points because they are decentralized. However, compared to infrastructure networks, mobile wireless networks are more susceptible to security risks. Securing a mobile wireless network is quite challenging because all networking tasks, such routing and packet forwarding, are carried out by the nodes themselves, just like in MANETs. It is important to take into account the increased risk of eavesdropping, spoofing, and denial-of-service attacks[10]. Due to the dispersed nature of security, routing, and host setup, there is no centralized firewall.

9. Limited Device: SecurityMANET devices are often portable and small, and they are not region-specific. This makes these gadgets susceptible to loss, damage, or theft. For short-range communications, they are employed. Therefore, nodes that want to connect with one another directly need to be close to one another. Multi-hop routing techniques are used to connect distant nodes via intermediary nodes that serve as routers in order to get around this restriction. Because they may be swiftly deployed without the assistance of a fixed infrastructure, MANETs can be employed in circumstances when temporary network connectivity is required.

10. Distributed Operation: Network control is dispersed among a number of nodes rather than being centralized throughout a background network. Each node in a MANET should work together and interact with the others, acting as an exchange when necessary to carry out particular tasks like routing and security [11].

11. Less Human Intervention: They are dynamically autonomous since setting up the network only requires a minimal amount of human participation.

1.1.3 Advantages and Disadvantages of MANET

Advantages:

1. Dissociation from centralized network management
2. Each node can function as a router and a host at the same time, illustrating its autonomy.
3. Self-configuring and self-healing nodes do not need human assistance.
4. Extremely expandable and ideal for multiple network hubs.

Disadvantages:
1. Due to numerous restrictions like noise, interference situations, etc., resources are limited.
2. Insufficient authorization resources.
3. Less protected against attacks due to poor physical security.
4. High latency, which means that data transit between two sleeping nodes is significantly delayed.

1.2. Internet of Things (IoT)

1.2.1 What is IoT?

Six billion people use 2G, 3G, 4G, LTE, wifi, Wimax, mobile broadband, and wired networks to access the internet in today's technological world. With the aid of these technologies, internet users can socialize, play games, access multimedia content, surf the online, send and receive emails, share information globally, and more. When communicating worldwide, a variety of physical objects can be employed to make work easier for people. To connect physical items with the digital world using a variety of networks and communication methods, the Internet of Things is utilized. This cutting-edge technology is a good answer in this situation.

In order to provide complete systems for the good or service, the Internet of Things (IoT) is a sophisticated automation and analytics system that works with artificial intelligence, sensor, networking, electrical, and cloud messaging, among other things. IoT-made systems have improved performance, control, and transparency. The Internet of Things interacts with wireless sensor networks (WSN) and mobile ad hoc networks (MANET) in smart settings, increasing its user appeal and commercial viability.

The creation of new MANET-IoT systems and IT-based networks is made possible by the interaction of wireless sensors and ad hoc mobile networks with the Internet of Things. This kind of solution reduces the expense of network deployment while increasing user mobility. However, it also brings up brand-new, challenging difficulties in relation to networking.

We can connect everything around us because we have a platform that holds all the data, like the cloud. Consider a home where we can connect all of our appliances—such as lighting, air conditioners, and other fixtures—through each other and control them all from a single platform. We have a platform that allows us to link our car and monitor its position, speed, and fuel level [3].

1.2.2 How does the Internet of Things (IoT) Work?

Depending on the IoT echo system, the operation of IoT differs (architecture). However, their fundamental operating concepts are comparable. The gadget itself, such as smartphones, digital watches, and electronic appliances, which securely connect with the IoT platform, is the foundation of the Internet of Things. Applications are used to convey the most useful data from platforms to devices after they have collected and analyzed data from various devices and platforms [4].

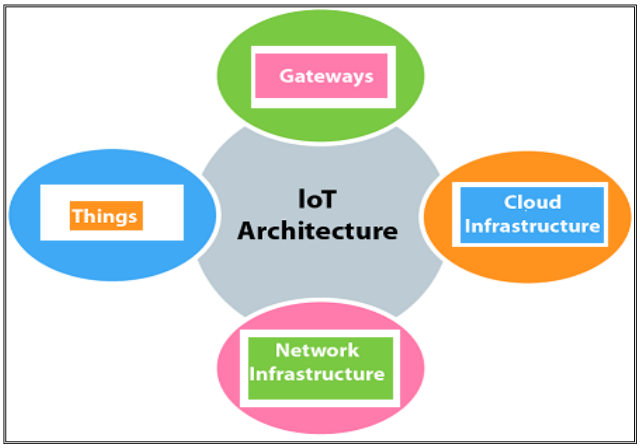

Figure 2: Working Process of IoT

1.2.3 Level Features of IoT

1. Sensing complex environment:
New techniques for gathering and sending information from the real world to a database have been invented.

2. Product identity management:
IoT should be able to recognize products in the cloud given the presence of the internet. To tailor dynamic data for any goods with allowed apps and nodes, it should use a flexible data storage.

3. Power is critical:
The same characteristic also enables MANET to focus. Since many IoT applications must run for years on batteries, less energy is used overall. The intricacy of the Internet of Things: Any professional should be able to develop an IoT application that uses information from databases or the cloud. Real-time data management is necessary for many services, as is the deployment of applications.

4. In-depth analytics and insights:
Products that are smarter have comprehension and insight. Real-time analytics and IoT data sharing with your company.

5. Cloud-to-cloud or database-to-database connectors:
Connectors that enable the interchange of information or data from physical items are necessary since it is very challenging to manage all of the data from the IoT's global value chain in a single cloud or database.

6. Connectivity:
The IoT's connectivity is its lifeblood. Connectivity is the creation of a link between several objects (also known as nodes) so they can talk to one other independently. The interaction and communication between numerous gadgets, sensors, computers, and data buses is necessary for the Internet of Things. IoT cannot be used in business without a quick, secure, and safe connection. Utilizing cross-domain technology like blockchain, AI, and cloud computing, IoT also links devices. Radio waves, Wi-Fi, Bluetooth, or cables can be used to connect them.

7. Scalability:
IoT systems are made to allow for easy scaling up and down of the number of devices, sensors, or computers as required. An IoT system should be flexible enough to handle workload during periods of high demand and resume regular operation during periods of low demand.

8. Sensing:
IoT devices collect and analyze data about their environment, including temperature, light, sound, acceleration, and pressure, before making a decision. As a result, sensors help automate processes by acquiring data and carrying out tasks that would often be handled by humans. The base of IoT operation is made up of the raw data that is gathered and evaluated. For instance, sensors like radar sensors and optical sensors might gather information in an autonomous door. It opens the door on its own if it senses someone approaching. Some sensors used in IoT include humidity sensors, temperature sensors, accelerometers, gyroscopes, motion sensors, image sensors, level sensors, and proximity sensors.

9. Analysing:
We are aware that IoT uses sensors to collect raw data, but why does IoT need data? What uses does the Internet of Things make of all that unprocessed information? Data is worthless in and of itself. Unless data is actively processed to provide insightful conclusions, it is meaningless and useless. IoT gathers unprocessed data in order to make sense of it. Because raw data can be highly helpful if processed appropriately, it is vital to analyze it in terms of structure, correlation, and usability. For instance, the robotic door stated earlier should be able to discriminate between a person and an animal after analyzing sensor data.

10. Artificial Intelligence:
The Internet of Things (IoT) gains significantly greater use when integrated with AI. Your smart refrigerator, for instance, can remind you to stop at the store on the way home if you run out of groceries. Thanks to artificial intelligence, things like this are now feasible. IoT devices collect raw environmental data and transform it into something interesting and helpful. In order to help them comprehend and function better in their settings, IoT devices and systems are also educated using a variety of machine learning models.

10. Smaller Device:
The size of tools and machinery (such semiconductor chips and sensors) is getting smaller. Precision and performance are provided by these little devices in the Internet of Things. It's incredible to believe that such tiny things can accomplish so much and raise our standard of living (for example, small sensors can tell us the quality of air in that area, protecting us from pollution).

11. Dynamic Nature:
IoT systems must be dynamic in that they adapt to changes in their surroundings in order to be useful for business. Let's use an example to demonstrate this. A smart air conditioner should be able to adjust the room's temperature based on the weather outside using the temperature sensor data. Additionally, it must be able to modify the humidity inside the space in reaction to variations in the humidity outside.

12. Active Engagement
IoT products and gadgets are connected to cross-domain technologies like blockchain, AI, cloud computing, and so on. To gather and alter data for commercial objectives, various goods and technology must work actively together. Raw data is incredibly powerful and can greatly enhance business decisions. Because of this, active interaction between different IoT products and these technologies is crucial.

13. Integration
IoT combines numerous cross-domain technologies, including cloud computing, AI, big data, and deep learning, to give users a delightful experience. The internet of things has changed to become the internet of everything. It is no longer only the internet of things. Our quality of life is greatly enhanced by a complete ecosystem of integrated gadgets.

14. Automated
Automation is a feature of every technology. Automation is the core tenet of the Internet of Things. IoT was developed to automate tasks and improve people's lives and enterprises; for instance, an IoT farming system automates watering while simultaneously reducing water wastage.**15. Security**

Security is one of the main issues that IoT users have. The security of the devices and the data flowing between them should be given priority because IoT systems store and transmit a lot of sensitive data. When developing an IoT system, appropriate security and safety measures are applied to prevent a security compromise. IoT systems demand significant resources and investment to assure their safety and viability, but these requirements must be met. Failure to do so would lead to distrust among its customers and companies, which would lower demand.

16. Endpoint Management
An IoT that has been carefully developed and implemented is a useful resource in the commercial world. IoT systems' endpoint management, however, is crucial; without it, the system as a whole could fail. Let's imagine that when you run out of food, your smart fridge orders some from a store. Food waste and an IoT failure could occur if you are away from home for a few days. Endpoint management is thus a necessary component of the Internet of Things [5].

1.2.4 Internet of Things interaction with MANET and WSN
The interoperability of various communication technologies and networks in smart environments is directly related to the potential for widespread deployment

of Internet of Things systems in numerous industries. Humans are becoming more dependent on remote monitoring of various processes in intelligent environments as the number of sensors rises. The growing use of wireless sensor networks enables this (WSNs).

WSN is essentially a network of different sensors that can handle detected data, temporarily store it, and transport it to another network node that is itself a sensor. These sensors can independently read information from the object being monitored. The central node, also known as the sink, receives data sensed and relayed from other sensors because WSN is often a centralized network. Wireless sensor networks in IoT systems now have a wide range of potential applications since wireless sensors can communicate with one another [5]. (WSNs).

The worldwide Internet of Things system is built on wireless sensor networks because sensors may gather data from many sources and send it across the network. On the other hand, the scalability and power consumption of WSN have a significant impact on the reliability of IoT systems [6]. The sensors must communicate measured data to the sink as effectively as possible to get the most out of their battery power. So that it can easily adapt to network changes, the wireless sensor network should be restricted. Since low or depleted batteries kill sensors, this is also related to the longevity of WSNs.

Because data must be conveyed by another sensor, eliminating dead sensors from the routing channel, routing principles and methods in WSN are a vital and demanding subject. Additionally, Quality of Service (QoS) across wireless sensor networks should be considered [7].

Wireless sensor networks and Mobile Ad Hoc networks are comparable in that both are self-organized and multi-hopped networks (MANET). WSN topology is less flexible than MANET topology, nevertheless. Its ability to function as a WSN backbone [8], access wireless sensor network nodes, and communicate with WSN about its entry points is made possible via MANET protocols.

The task of utilizing sensors' energy efficiency during data transmission and decreasing data processing time by choosing appropriate routing protocols and principles calls for the convergence of MANET and WSN networks.

These two networks can also make cross-network routing more efficient and dependable in the context of the Internet of Things. A MANET-IoT system is the confluence of MANET, WSN, and the Internet of Things. The key relationships between the Internet of Things, wireless sensor networks, and mobile ad hoc networks are shown in Figure 3.

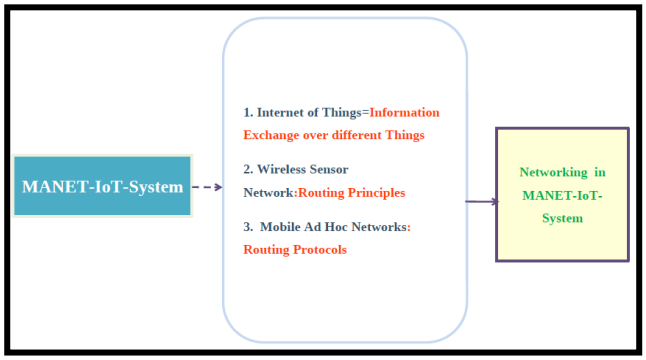

Figure 3: Interaction of IoT, WSN, and MANET

The MANET-IoT system's networking is based on wireless sensor network routing concepts, MANET routing protocols, and Internet of Things-based data handling, processing, and sensing from things. In terms of routing, networking such a system is generally very challenging. The limited resources of all network sensors and the mobility of the system are also relevant. Routing in wireless sensor networks is centered on network node energy efficiency, and the majority of MANET protocols are created with QoS in mind [10, 11].

The MANET-IoT system's connectivity, accessibility, and dependability in smart environments must be ensured through the connection of diverse items with limited features to the Internet as well as interaction with various wireless and Mobile Ad Hoc networks. To fulfill the needs of the Internet of Things, Tian and Hou [12] provided solutions for Ad Hoc network modification routing protocols. Routing rules were modified by introducing IPv6 [13]. However, a novel, efficient method for data routing in such a MANET-IoT system is required by the interaction of the Internet of Things with MANET and WSN.

II. ROUTING PROTOCOLS IN MANET

This section describes the various types and classifications of wireless ad hoc routing protocols that are currently in use. Depending on how routing information is updated, there are three different types of routing protocols for ad hoc wireless networks. They can be on-demand (reactive), table-driven (proactive), or hybrid [14–23].

The several proposed Ad hoc routing techniques for each of the three categories are shown in Figure 4. The connectionless approach of packet forwarding is similar to the table-driven ad hoc routing method in that it disregards when and how frequently such routes are requested.

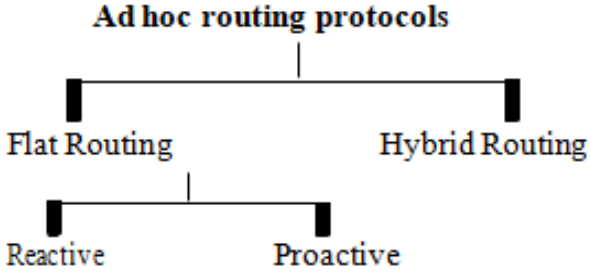

Figure 4: Routing Protocols in MANET

Routing rules were modified by introducing IPv6 [13]. However, a novel, efficient method for data routing in such a MANET-IoT system is required by the interaction of the Internet of Things with MANET and WSN.

I. IoT-Enabled Proactive Routing Protocols

The routes that link each node to the other nodes in the network are continuously tracked by these protocols. By communicating topological information between network nodes, these protocols continuously learn the topology of the network. This means that when a route to a place is needed, the information about the route is readily available. Various route states are tracked by various protocols [18]. Popular proactive routing techniques are discussed in the following section

A. Destination-Sequenced Distance-Vector (DSDV)

The Perkins and Bhagwat-recommended protocol (DSDV) [14] is a vector that shows the distance between two places.

The Bellman-Ford Routing Algorithm served as the foundation for the routing protocol, while several changes were made to make it loop-free, for example.

Distance vector routing is less reliable than link state routing due to count to infinity problems and the bouncing effect.

The routing protocol was built on the Bellman-Ford Routing Algorithm with a number of modifications, such as making it loop-free.

Due to issues with count to infinity and the bouncing effect, distance vector routing is less trustworthy than link state routing.

Some improvements, such removing loops Count to infinity issues and the bouncing effect make distance vector routing less dependable than link state routing. In this case, each device keeps a routing table containing entries for each other linked device. In order to keep the routing database completely up to current at all times, each device frequently broadcasts routing messages to its neighbors. A neighbor device compares this value to the corresponding value stored in its routing table after knowing its current link cost and receiving the broadcasted routing message. If changes are made, the value is updated, and the distance computation for the route using this link in the routing table is amended [20].

B. Wireless Routing Protocol (WRP)

The Bellman-Ford Algorithm is inherited by WRP, a table-based protocol similar to DSDV that was developed by Murthy and Garcia-Luna-Aceves [18]. The main goal is to track the routing data for the shortest path between each destination and each network node. By requiring each node to perform consistency checks on preceding data provided by all of its neighbors, it is a path-finding strategy that leverages a loop-free wireless routing protocol to get around the count-to-infinity problem.

The Distance table (DT), the Routing table (RT), the Link-cost table (LCT), and the Message retransmission list (MRL) are a collection of four tables that each node in the network utilizes to maintain more exact information (MRL). When a link between two nodes fails, the neighbors are updated. With one crucial exception, WRP belongs to the class of path-finding algorithms. It solves the count-to-infinity issue by requiring each node to confirm the accuracy of previous data reported by all of its neighbors. In the event of a link breakdown, this avoids looping and provides faster route convergence. [18]

C. Optimized Link State Protocol[OLSR]

Clausen and Jacquet[18] proposed the OLSR, a proactive point-to-point protocol that takes advantage of multipoint relaying, a successful link state packet forwarding method. The simple link state routing approach is improved by it. The two methods of optimization are lowering the quantity of control packets and the quantity of links needed to transmit link state messages. Each node in this system maintains the network topology information by periodically exchanging link-state messages with the other nodes. OLSR is supported by three mechanisms: neighbor sensing, efficient flooding, and shortest-path algorithm-based computation of the optimum path. In order to determine the optimum path, the shortest path algorithm is then applied. Routes to each destination are immediately available and valid once data transmission begins.

D. Fisheye State Routing (FSR)

Pei and others. [20] A graphic information compression technique based on the "fisheye" method created by Kleinrock and Stevens is the FSR protocol. The quantity of data maintained by this approach decreases with increasing distance from the node, but it does preserve accurate distance and path-quality information about a node's close surroundings. A few nearby fisheye scopes, or places reachable in one, two, or more hops, are taken into account by each node. FSR reduces the number of update messages by updating network data for nearby nodes more frequently than for distant nodes outside the fisheye scope. As a result, FSR is more scalable to large networks than protocols.

Table 1: Comparison of IoT-enabled Proactive Routing Protocols

Parameters	DSDV	WRP	OLSR	FSR
Route updates	Periodic	Periodic	Periodic	Periodic
Loop free	Yes	Yes	Yes	Yes
Routing overhead	High	High	Low	High

Caching overhead	Medium	High	High	Low
Throughput	Low	Low	Medium	High
Routing tables	2	4	4	4
Update Destinattionion	Neighbor	Neighbor	Neighbor	Neighbor and Clusterhead
Hello Message	Yes	No	No	No
Multiple Routes	No	Yes	No	No

III. REACTIVE PROTOCOLS

Reactive or on-demand routing systems are based on the Query-Reply topology and do not make an attempt to continuously maintain the network's topology current, in contrast to proactive routing protocols. A procedure to find a path to the required node is begun when a route is required. Reduced network traffic overhead is the primary goal of reactive or on-demand routing techniques. These routing strategies are built on "query-reply" conversations. They don't make an attempt to keep the network's topology up to date on a regular basis. Instead, a reactive protocol employs a procedure that entails barrages of route requests to the network to find a path to the target as the need arises. On-demand is a typical phrase for these protocols as a result.

The route discovery technique is a feature shared by all reactive protocols. From the source node to the destination node is transmitted a route request message. Until it reaches its destination, this message is flooded or relayed by all network nodes. If the intermediary or destination nodes have enough topological knowledge, they will send the sender a reply message that includes information about the route that the request message took. Consequently, a lot of reply messages might be sent, leading to a lot of different paths, of which the shortest one has to be utilized. [24] Reactive routing protocols include the following:

A. Ad hoc On-Demand Distance Vector Routing(AODV)

For use in ad hoc networks, C. E. Perkins and E. M. Royer[25] created the widely used on-demand routing protocol known as AODV. The DSR and DSDV are combined to create the AODV. Along with the essential on-demand DSR Route Discovery and Route Maintenance mechanism, it makes use of the hop-by-hop routing, sequence numbers, and periodic beacons of DSDV. It guarantees loop freedom at all times and allows quick convergence when the ad hoc network topology changes by overcoming the Bellman-Ford "count-to-infinity" problem. Since it only finds routes when they are needed, AODV is a reactive system. The fundamental flaws in AODV protocols are a deceptive decrease in hop count as well as a deceptive increase in sequence number.

The security of AODV is increased by Zapata [26] by using one-way hash algorithms to serve metric information in Route Request (Route Discovery). In order to authenticate non-mutable data end-to-end using digital signatures, he put up the Secure-AODV (SAODV) [27] concept. Hash chains are used to secure modifiable data such as hop count. It has enhanced the AODV Routing Protocol. It provides security features to safeguard the AODV Route Discovery method, including integrity, authentication, and non-repudiation. AODV doesn't perform local path fixes. Periodic beacons or ACK signals demonstrate that both the source and destination nodes are informed when a link fails (end nodes). The source node then reconstructs the destination and source node paths using higher layers. AODV does not.

- **Dynamic Source Routing (DSR)**

The on-demand protocol known as DSR was created by D. B. Johnson, Maltz, and Broch [25] to lessen the amount of bandwidth needed by control packets in ad hoc wireless networks. By eliminating periodic table update messages that proactive routing methods require, this protocol achieves its goal. By utilizing source routing, dynamic source routing can be identified. Since DSR is a reactive protocol, it doesn't require frequent updates. It determines the routes and then updates them as necessary. The sender of a packet specifies the entire network of nodes that the packet must flow through. This route is then explicitly listed by the sender in the packet's header, and each forwarding "hop" is identified by the address of the next node.

The DSR protocol is composed of the phases of route discovery and route maintenance. Every node has a cache of recently discovered paths. Before transmitting a packet, a node first makes that the cache contains a matching entry. If so, the message is sent using that route. The source address is also included in the packet. If there is no entry in the cache or if the entry has expired, the sender sends a route request packet to all of its neighbors to ask for a path to the destination.

The sender host keeps an eye out for the route. When the route request packet reaches any other node, it is checked to see if the stated destination is there. If they have any path information, they return a route reply packet to the destination. If not, a route request is broadcast in the same packet. Once the route has been determined, the sender will utilize it to send the required packets while also adding an entry to the cache for future usage. The node additionally keeps track of the entry's age in order to determine whether the cache is new or not. When an

intermediate node gets a data packet, it first decides if it was sent to itself.

- **Temporally Ordered Routing Algorithm (TORA)**

The distributed routing algorithm TORA [25] was created by Park and Corson and is highly adaptive, loop-free, and relies on link reversal. The pathways are classified as either upstream or downstream using directed acyclic graphs (DAG). TORA can now provide improved route assistance for networks with dense, massive node populations as a result of this graph [28]. ToRA, however, requires node synchronization to provide this functionality, which limits the utility of the protocol. TORA is a pretty sophisticated protocol, but what makes it unique is that when a link fails, it only propagates control messages in the vicinity of the failure.

All other protocols, however, must redo route discovery when a link breaks, while TORA can avoid this issue. With this capability, TORA can expand to larger networks, although doing so comes at a higher cost for smaller networks. Route creation, maintenance, erasure, and optimization are the four primary functions performed by TORA. Every node must have a height, therefore if one doesn't exist, the node is assumed to have been removed and its height is set to zero. To improve the link structure, nodes are occasionally given new heights. This operation is referred to as route optimization [25].

D. Associativity-Based Routing (ABR)

Degree of association stability is a new class of routing metrics introduced by the ABR protocol for mobile ad hoc networks. Depending on the degree of association stability of mobile nodes, a route is chosen in this routing system. Each node consistently generates a beacon to announce its presence. After receiving a beacon message, a neighbor node makes changes to its associativity table. The associativity tick between the receiving node and the beaconing node increases with each beacon received. Any beaconing node with a high associativity tick value is most likely to be a node with a low degree of dynamicity. When a neighboring node departs the vicinity of another node, the associativity tick is reset [26].

TABLE 2: Comparison Of IoT-enabled Reactive Routing Protocols

Properties	AODV	DSR	TORA	ABR
Route Creation	By source	By source	Locally	By Source
Multiple Routes	Yes	No	No	Yes
Route Maintainance	Routing Table	Route Cache	Route Table	Routing Table
Periodic updation	No	No	No	Yes
Performance Metrics	Speed	Shortness	Speed	Speed
Routing overhead	High	High	High	High
Caching overhead	Low	High	Medium	High
Throughput	High	Low	Low	High
Multipath	No	Yes	Yes	Medium
Route updating	Non-periodic	Non-periodic	High routing overhead	Periodic
Multicasting	Full	Full	Local	Full
Route Metric Method	Shortest Path	Shortest Path or Next Route Cache available	Shortest Path or Next available	Shortest Path
Topology	Full	Full	Reduced	Full
Complexity	02D	02D	02D	02D

IV. HYBRID ROUTING PROTOCOLS

Both proactive and reactive routing components are intended to be included in these protocols. They are widely used to provide hierarchical routing, which can generally be flat or hierarchical. All hybrid routing protocols struggle to determine the best configuration for the network given the network's characteristics. The only negative of hybrid routing approaches is often that nodes with high-level topological information have a tendency to keep more routing information, which consumes more memory and power [19]. Here are some examples of hybrid routing protocols:

A. ZRP

In their Zone Routing Protocol proposal, Haas and Pearlman. ZRP [40] is a hybrid routing system that leverages subnetworks as nodes for mobile ad hoc networks (zones). Combining proactive and on-demand routing systems' advantages, it. Each zone features proactive routing to improve neighbor interaction. To reduce useless communication, on-demand routing is used for inter-zone communication. The distances between mobile nodes are used to divide the network into routing zones.

A specific node, N, and all other nodes within d hops of N are referred to as being in the same routing zone. Its routing zone's nodes that are precisely d hops away from N are regarded as N's peripheral nodes. The size of the zone is a key consideration in zone routing. First described by [27], the enhanced zone routing technology known as Independent Zone Routing (IZR) allows for adaptive and distributed reconfiguration of the ideal zone size. The ad hoc network's scalability is further improved by the IZR's adaptability. The routing information on each node in the zone must be updated on a regular basis. Additionally, each node performs local route optimization, which includes connection failure detection, route shortening, and the removal of redundant pathways.

B. Zone-based Hierarchical Link State routing(ZHLS)

The size of the zone is a key consideration in zone routing. First described by [27], the enhanced zone routing technology known as Independent Zone Routing (IZR) allows for adaptive and distributed reconfiguration of the ideal zone size. The ad hoc network's scalability is further improved by the IZR's adaptability. The routing information on each node in the zone must be updated on a regular basis. Additionally, each node performs local route optimization, which includes the removal of duplicate pathways, route condensing, and link failure detection similar to node-level link state information.

The source node confirms its intra-zone routing table prior to transmission. The route information is already available if the destination falls inside its zone. In every other scenario, the source employs gateway nodes to send a location request to each and every zone, and each zone responds with a location response that includes the zone ID of the desired destination. Data packets arriving from the source contain the zone ID and node ID of the destination node in the header. In comparison to AODV and DSR, ZHLS has a low overhead for routing. The routing path can also be modified to fit the dynamic topology since only the node ID and zone ID are required for routing. As a result, as long as the destination is still within the zone, no additional search is needed [28].

C. Distributed Spanning Trees (DST)

The network's nodes are structured into a variety of trees [29]. There are two different types of nodes in each tree: route nodes and internal nodes. The root of each tree determines the structure of the tree and whether it can merge with another tree. The remaining nodes inside each tree are regular nodes. Depending on the task it is attempting to do, each node may be in one of three states: router, merge, or configure. For selecting a path between a source and a destination pair, DST advises using the following two techniques: A hybrid tree flooding technique With this method, every nearby bridge and spanning tree receives control packets broadcast from the source.

Each package is stored at these places for a defined amount of time. Based on Distributed Spanning Trees (DST), Shuttling: In this technique, the source disperses control packets to the edges of the tree until each one reaches a leaf node. Once a packet reaches the leaf node, it is sent on to the following level of the network. The disadvantage of such a design is that the entire tree has a single point of failure. The entire routing topology falls apart if the root node malfunctions. The holding time required to buffer the packets may also add additional network latency.

D. DDR

Nikaein et al. [30] offer a tree-based routing scheme that does not require a root node. This strategy tree is built using periodic beaconing messages that only neighboring nodes can exchange. The newly formed gateway nodes connect the network's trees, which collectively form a forest. These gateway nodes consist of regular nodes from various trees which are close in transmission. A unique zone ID is assigned to each tree in the network using the zone name technique. The network as a whole is now filled with several zones that overlap.

The DDR algorithm contains six phases: preferred neighbor selection, intra-tree clustering, inter-tree clustering, forest construction, zone naming, and zone partitioning. HARP, or hybrid ad hoc routing protocols, is used to choose routes [45]. The intra-zone and inter-zone routing tables of DDR are used by HARP to identify a stable route between the source and the destination. While DDR offers the advantage of not relying on a static zone map for routing, ZHLS requires a root node or cluster head to coordinate data and regulate packet delivery between various nodes and zones.

E. Scalable location updates routing protocol (SLURP)

This process, which is similar to ZLHS in SLURP [31], The nodes should be placed so that they are visible in a variety of non-overlapping zones. But by limiting network-wide global route discovery, this protocol (SLURP) considerably reduces the cost of maintaining routing information. To support the achievement of this attribute, a home area is assigned to each network node. When a data packet reaches the location of the destination, it is routed there using source routing4. SLURP's main flaw is that it depends on an already-programmed static zone map (as does ZHLS).

TABLE 3: Comparison of IoT-Enabled-Hybrid Routing Protocols

Parameters	**ZRP**	**ZHLS**	**DST**	**DDR**	**SLURP**
Routing g Structure	Flat	Hierarchical	Hierarchical	Hierarchical	Hierarchical
Multiple routes	No	Yes	Yes	Yes	Yes
Beacon s	Yes	No	No	Yes	Yes
Route information stored	Intrazone & Interzone tables	Intrazone & Interzone tables	Route tables	Intrazone & Interzone tables	Intrazone & Interzone tables
Route metric	Sho1test path	Sho1test path	Forwarding using the tree	Stable routing	Shortest Path
Advantage	Reduced transmissions	Low control overhead	Reduced transmission	No zone coordinator or zone map	No zone Coordination
Disadvantage	Overlapping zones	Static zone map required	Root node	Neighbors may become bottlenecks	Static zone mapping

TABLE 4: Comparison between the Three Categories of IoT-Enabled Routing Protocols

PARAMETER	**PRO-ACTIVE PROTOCOLS**	**REACTIVE PROTOCOLS**	**HYBRID PROTOCOLS**
Storage Requirements	Higher	Depends on the Number of Route maintained or needed	Depends on size of each zone or cluster
Route Availability	Always available	Computed as needed	Depends on location of destination
Periodic Updates	Required always some may use conditional	Not required but some may use Periodic beacons	Used inside each zone of the network
Route Delay	Low	High	Low for local Destinations (intra-zone) and high for Inter-zone
Scalability	100 Nodes	>100	> 1000
Control Traffic	High	Low	Lower than other two types
Routing Information	Keep stored in Table	Doesn’t store	Depends on requirement
Routing Structure	Mostly flat and Hierarchical	Mostly Flat	Hierarchical
Overhead Control	High	Low	Medium
Bandwidth	High	Low	Medium
Energy Requirements	High	Low	Medium

V. CONCLUSION

We explored routing in mobile ad hoc networks combined with IoT technology and gave comparisons between various IoT-enabled routing methods in mobile ad hoc networks. Source-initiated (reactive or on-demand), table-driven (pro-active), and hybrid protocols are the three categories into which the protocols are divided. We looked at and contrasted a few typical protocols from each of these classes using different criteria for network performance evaluation. Each routing protocol has its own set of characteristics, even if there are still many routing problems for mobile ad hoc networks. The right routing protocol must be chosen based on the IoT infrastructure and network conditions. The examination of the numerous recommendations showed that the intrinsic qualities of ad hoc networks, such as a lack of infrastructure and quickly changing typologies, add to the already difficult challenge of their insightful suggestions and knowledgeable comments that will enhance the paper's contents.

REFERENCES

[1] A. K. Gupta and H. Sadawaiti, "Secure Routing Techniques for MANETs, " *"International Journal of Computer The01y and Engineering"*, vol. **1**, **pp. 456-460, 2019**.

[2] C. E. Perkins, "Ad hoc Networking", *Pearson Publication*, **2015**.

[3] M. Rath, U.P. Rout, "Analysis and Study of Security Aspect and Application-Related Issues at the junction of MANET and IoT", *International Journal of Research in Engineering and Technology*., **2015.**

[4] Y. Tian, R. Hou, "An Improved AOMDV Routing Protocol for Internet of Things", *International Conference on Computational Intelligence and Software Engineering (CiSE)*, **2010.**

[5] N. Bessis, F. Xhafa, D. Varvarigou, R. Hill, M. Li, "Internet of Things and Inter-cooperative Computational Technologies for Collective Intelligence", *Berlin: Springer-Verlag*; **2013**.

[6] M. Potnuru, P. Ganti, "Champaign. Wireless Sensor Networks: Issues, Challenges, and Survey of Solutions", *International Journal of Computer Science Engineering*, **2016.**

[7] B. Bhuyan, H. Kumar Deva Sarma, N. Sarma, A. Kar, R. Mall, "Quality of Service (QoS) Provisions in Wireless Sensor Networks and Related Challenges*". Wireless Sensor Network*, **2018.**

[8] M. Rath, U.P. Rout., "Analysis and Study of Security Aspect and Application-Related Issues at the junction of MANET and IoT", *International Journal of Research in Engineering and Technology*, pp. **426–430, 2015**.

[9] A. Boukerche, B. Turgut, N. Aydin, M.Z. Ahmad, L. Bölöni, D. Turgut, "Routing Protocols in Ad Hoc Networks: A Survey", *Computer Networks*, **2017**.

[10] L. Hanzo, R. Tafazolli., "A Survey of QoS Routing Solutions for Mobile Ad hoc Networks", *IEEE Communications Surveys & Tutorials.* **2017.**

[11] K. Akkaya, M. Younis, "A Survey on Routing Protocols for Wireless Sensor Networks" *Ad Hoc Networks*., **2015**.

[12] Y. Tian, R. Hou, "An Improved AOMDV Routing Protocol for Internet of Things", *International Conference on Computational Intelligence and Software Engineering (CiSE)*, **2020.**

[13] T. Tsvetkov. "RPL IPv6 Routing Protocol for Low Power and Lossy Networks". *Network Architectures and Services*, **2011.**

[14] A. K. Gupta, H. Sadawaiti, and A. K. Verma, "A Review of Routing Protocols for Mobile Ad Hoc Networks*", SEAS Transactions on Communications"*, **2011.**

[15] P. Papadimitratos and Z. J. Haas. "Secure routing for mobile ad hoc networks," *SCS Communication Networks and Distributed Systems Modeling and Simulation Conference*, **2012.**

[16] M. Zapata, N. Asokan, "Securing ad hoc routing protocols *", WiSe '02, ACM,* **2012.**

[17] E. M. Royer and Chai-Keong Toh, "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks*", SEAS Transactions on Communication*, **2021.**

[18] N. S. Yadav and R.P. Yadav, "Pe1formance Comparison and Analysis of Table- Driven and On-Demand Routing Protocols for Mobile Ad hoc Networks," *"International Journal of Information Technology'*', **2017.**

[19] A. Boukerche, B. Turgut, N. Aydin, M. Z. Ahmad, L. Boloni, and D.Turgut, "Routing protocols in ad hoc networks: A survey," *Elsevier Computer Networks'*,**2022..**

[20] C. E. Perkins and P. Bhagwat, "Highly Dynamic Destination Sequenced Distance-Vector (DSDV) for Mobile Computers," *Proc. ACM Conf Communications Architectures and Protocols"*, **2014**.

[21] T. H. Clausen et al., "The Optimized Link-State Routing Protocol. Evaluation through Experiments and Simulation," *"Proc. IEEE Symp. Wireless Personal Mobile Communications*, **2021**.

[22] S. Mmthy, C. Siva Ram and B.S. Manoj, *"*Ad Hoc Wireless Networks: Architectures and Protocols,*" Prentice Hall, Chapter 7*, **2014.**

[23] T. A.Wysocki, A. Dadej, and B. J. Wysocki, "Secure routing protocols for mobile ad-hoc wireless networks," *"inAdvanc ed Wired and Wireless Networks", Eds. Springer*, **2014**.

[24] A. A. Pirzada, C. McDonald and A. Datta, "Pe1formance Comparison of bust-based Reactive Routing Protocols," *"IEEE Trans. Mobile Computing"*, vol. **5**, issue **6**, **2016.**

[25] A. K. Gupta, H. Sadawaiti, and A. K. Ve1ma, "Pe1formance analysis of AODV, DSR & TORA Routing Protocols," *"IACSJT International Journal of Engineering and Technology"*, vol.**2**, April **2020**.

[26] Raja, J., & Santosh, S. , "Comparative study of reactive routing protocol (AODV, DSR, ABR, and TORA) in MANET", *IJECS*, **2022.**

[27] P. Samar, M. R. Pearlman, and Z. J. Haas, "Independent zone routing: an adaptive hybrid routing framework for ad hoc wireless networks," *"in IEEE/ACM Transactions on Networking (TON)"*, **2015.**

[28] T. Hamma, T. Katoh, B. B. Bista and T. Takata, "An Efficient ZHLS Routing Protocol for Mobile Ad Hoc Networks," *17th International Workshop on Database and Expert Systems Applications*, **2016.**

[29] S. Radhakrishnan, N. Rao, G. Racherla, C. Sekhai·an, and S. Batsell, "DST – a routing protocol for ad hoc networks using distributed spanning trees," in: *"Proceedings of IEEE WCNC "*, **September 2019.**

[30] N. Nikaein, H. Labiod, and C. Bonnet, "DDR: distributed dynamic routing algorithm for mobile ad hoc networks," in: *"Proceedings of ACM MobiHoc* ", **August 2020.**

AUTHORS PROFILE

Dr. GATETE Marcel, Doctor of Philosophy degree, Periyar Maniammai University, India 2012-2018, Master of Philosophy PRIST University, India 2010-2011, M.SC. Bharathidasan University, India 2008-2010, B.SC., Institutut Superieur Pedagogique de Gitwe, Rwanda 2002-2006. Lecturer in the department of Computer Science, University of Gitwe, Rwanda. Interested Area: Mobile Ad Hoc Networks and Computer Programming.

HARUBWIRA Flaubert, Mr. Flaubert HARUBWIRA , Master's in Information Technology, University of Bharathidasan , Bishop Heber College, India 2011-2013, Master's in M.com Banking and Insurance Management, Annamalai University, India 2012-2013.; University of Gitwe , Bachelor of Computer Engineering Rwanda 2003- 2007. Dean of the faculty of Business and Information Technology in UTB (University of Tourism, Technology and Business Studies, \

