INJ INTERNATIONAL NEUROUROLOGY JOURNAL

Testing and Evaluation of the Routing Protocol's effectiveness for LLNs : An Analysis and Study – Part II

Dr. Anitha T.N., Thrisha V.S., Dr. Mamatha C.M

Professor & Head, Department of Computer Science & Engineering, Sir. M Visvesvaraya Institute of Technology, Bangalore, India

Assistant Professor, Department of Computer Science & Engineering, Sir. M Visvesvaraya Institute of Technology, Bangalore, India

Professor and Head, Dept. of Computer Science & Engineering (CY), Cambridge Institute of Technology North Campus, Bengaluru, Karnataka

Abstract

The abstract is already presented in the previous part-I of the same article titled, Testing and Evaluation of the Routing Protocol's effectiveness for LLNs : An Analysis and Study – Part I.

Key Words: RPL, LLN, Objective Function, MRHOF, OF0, AODV, QOS, LVMP.

Introduction

The paper is an extension of the previous paper by the same authors titled, "Testing and Evaluation of the Routing Protocol's effectiveness for LLNs : An Analysis and Study – Part II". Here, follows a brief survey of the same.

In the ref. [14] Intercommunication in Packet Network Protocol, the sharing of resources between various packet switching networks is supported by a certain protocol. The protocol supports end-to-end error checking, sequencing, flow control, changes in individual network packet sizes, transmission failures, and the establishment and deletion of logical process-to-process links. Considerations are made for several implementation challenges, and issues with accounting, timeouts, and network routing are revealed. In our discussion of the connectivity of packet switching networks, we covered some important topics. We have detailed a straightforward yet very robust and adaptable protocol that allows for the modification of individual network packet sizes, transmission errors, sequencing, flow management, and the formation and dissolution of process-to-process relationships. By considering some of the implementation-related concerns, we discovered that HOSTS with significantly different capacities may implement the proposed protocol. The creation of a comprehensive specification for the protocol is a crucial next step, allowing for the execution of certain first tests. These tests are required to establish some of the operational characteristics of the proposed protocol, such as the frequency and extent of packet arrival out of order, the amount of segment acknowledgment delay, and the appropriate retransmission timeouts.

[15] Network Throughput, End-to-End Delay, and Normalized Routing Overhead Comparative Study of Two Routing Protocols We propose a simulation-based study to place a value on the necessity of a cross-layer project for enhanced QoS sustenance in radiocommunication Adhoc networks. Using the J-Sim simulator, we contrast the CROSS-LAYER Engine architecture's use of the QoS-PAR direction-finding procedure with the coated construction's use of the AODV routing protocol. Due to its suitability for cross-layer implementations, we employ J-Sim. In addition to the suggested routing protocol, QoS-PAR , and the LYMP protocol, we used it to create the whole CROSS LAYER Engine architecture. In contrast to AODV, whose performance declines noticeably as network size or the number of accepted flows increases, QoS-performance PAR's was also virtually unaffected by these factors. If we compare QoS-PAR over CROSS LAYER Engine with AODV over the layered building, the performance of AODV degrades substantially when the network size or the number of flows is raised while that of Position Assisted Routing Protocol was not sensitive to either.

[16] Wireless Sensor Networks: Routing Protocols and Security Issues, the author of this study holds that a wireless network made up of a lot of sensor nodes is the Wireless Sensor Network (WSN) . Network communication is facilitated by routing protocols. Routing protocols establish and keep up the routes in the network by determining the best way for data transmission. There have been several suggested routing methods for WSNs. Yet, these protocols can only be used to a certain extent without security. Another key aspect is ensuring safe communication between nodes This study analyses routing protocols' categorization and comparison. Furthermore, covered in this research are different security risks to wireless sensor network routing methods as well as a few countermeasures. The architecture of the routing protocols utilized in the wireless

DOI: 10.5123/inj.2023.4.in145

sensor network is also attempted to be clarified. Yet, the security of routing protocols falls short of our expectations in terms of security. Protection against attacks in WSNs requires network layer encryption and authentication.

[17] Performance Evaluation of Routing Protocols for MANETs under Different Traffic Conditions, in this article, it is shown how the flexibility of bulges in a movable Adhoc system causes frequent changes in the network architecture, creation direction-finding in MANETs a difficult operation. In terms of together presentation and dependability, the effective routing protocols can provide mobile ad hoc networks several advantages. There have already been several routing protocols suggested for these networks. Studies analyzing the recital of suggested direction-finding procedures below CBR traffic under various net circumstances have been described in the literature, but less attention has been paid to assessing their presentation when practical to circulation producers other than CBR, such as FTP, TELNET, etc. In contrast to CBR traffic, which does not accurately depict the multifaceted countryside of traffic in actual requests, these circulation states are more like the system demands that would be imposed on real-world MANETs. In terms of throughput, average end-to-end delay, packet delivery ratio, and routing message overhead, this article compares the presentation of three routing protocols—AODV, DSR, and WRP—for FTP, TELNET, and CBR traffic. A variety of network circumstances are considered, including the impact of changing the pause duration, the quantity of source-destination pairs (i.e., the provided load), and the normal node rapidity.

[18] Implementation DSDV routing protocol for wireless mobile ad-hoc network, using NS-2 simulator, Due of the extremely dynamic environment, routing in MANET is the focus of this research. Every time a packet needs to be transported to its terminus across many protuberances, a routing protocol is required, and numerous direction-finding methods consume stood suggested for ad-hoc networks. In this study, we attempt to compare the effects of responsive and practical kind etiquettes by increasing the node density in the system, keeping the source node fixed and moving the destination node, and ultimately keeping the destination node fixed and moving the source node. In each of the three scenarios, the routing protocol's effectiveness has been examined in order to enhance, choose, and create an effective routing protocol for network configuration and realistic situation. Packet loss, delivery fraction, and end-to-end latency are all included in the performance matrix. In terms of node mobility and network node density growth, this article realistically compares the three routing protocols DSR, AODV, and DSDV. Keep the basis bulge constant and the terminus protuberance variable in the first case. In comparison to AODV and DSDV, the performance of the DSR routing protocol is relatively good. In each of the three scenarios, the routing protocol's effectiveness has been examined in order to enhance, choose, and create an effective routing protocol for network configuration and realistic situation. Packet loss, delivery fraction, and end-to-end latency are all included in the performance matrix. In terms of node mobility and network node density growth, this article realistically compares the three routing protocols DSR, AODV, and DSD. Keep the basis bulge constant and the journey's end protuberance variable in the first case. In comparison to AODV and DSDV, the performance of the DSR routing protocol is relatively good.

[19] Analysis of Routing Protocols in an Emergency Communications Center, the focus of this essay is Routing protocols are cast-off in every network to select the most ideal routes for sending and receiving packets between different sites. An imagined rational system for a cooperative Emergency Communications Center (ECC) between two towns is presented in this study, which routing protocol offers the optimum speed and amount in a mission-critical situation must be assessed in order to consolidate and centralize the public safety network's essential functions. Convergence, throughput, and queuing time are tested for four different routing protocols: Routing Information Protocol, Open Shortest Path First, Interior Gateway Routing Protocol, and Improved Interior Gateway Routing Protocol. The net is modelled in Riverbed Modeler Academic Version 17.5 for Windows. Which procedure to be used may be determined by analyzing the findings. The direction-finding procedure to deploy in a net that is crucial to operations has been determined after a comprehensive examination and contrast of the chosen routing protocols. In almost every measurable metric, EIGRP consistently performed better than the other three protocols. File attendant packages to the ECC switch were the only circumstance in which EIGRP was assessed to perform better than the other three protocols. The margin by which EIGRP beat the other routing protocols was substantial, given how crucial database access and traffic are to a public safety network. The speed of convergence is a crucial component of every network. In a network for public safety, when seconds count, this is extremely important. The decision here was EIGRP without a doubt. Although it would be logical to think that no new networks would be developed using FDDI because it is an obsolete technology, many public safety groups lack the funding and technological know-how that a private company could have. Despite this, EIGRP remains the ideal protocol to employ because it experienced the least amount of latency.

[20] Proposed Routing Protocol for clouds, As the name indicates, the cloud that serves as a platform for numerous online services is what we refer to as the "cloud computing" in this study. The cloud is a representation of the pay-per-use model used for internet-based services. Open-source routing protocols are frequently used in the cloud. Also compatible with our cloud system is a wireless sensor network. A network is all that the cloud is, and it provides a variety of services, but in order to do so, a good network setup and packet transmission must be done. Several routing protocols are needed in order to transport a packet. The study compares routing systems based on network efficiency. One of the primary problems is how communication can be carried out via a wireless network on the cloud. The fundamentals of the various routing protocols used in networking were covered in this essay. A suggested protocol is provided for a cloud network that really has greater advantages in the clouds. Although each of the described routing protocols has a unique set of benefits, they all have the disadvantage of requiring a protocol that is both scalable and mobile in order to support big networks and mobile technologies. Since the source node searches for its destination's neighbors, this strategy practically minimizes network congestion while also assisting in a decrease in the frequency of broken links. There is no doubt that this strategy should be used as it doesn't need a lot of labor.

Proposed Research Methodology

In terms of packet forwarding, the node is egocentric. No matter if it is a data packet or a routing pack, it drops every pack it gets. According to expectation, a lower packet delivery ratio and thus a lower throughput are attained on nodes that are more selfish. While there is a tendency for the delay to decrease, it is to be anticipated that the delay will increase if the routing packets are lost. The packet was discarded more quickly the smaller the latency was (compared to the value received for a healthy network). The Fig. 8 gives the structure of the UAV communication network simulation system.

These two performance indicators are heavily influenced by the number of selfish nodes since fewer packets signify less network congestion and faster packet delivery can imply greater performance. AODV has a higher packet delivery rate than the other two protocols. There is more routing burden when there is suspicion about network activity. The load eventually abruptly lowers as a result of more routing packets being discarded by egotistical nodes than AODV, which responds more quickly to network changes and generates more control packets. The quantity of routing information sent by OLSR and DSDV, which both transmit recurrent updates, is the same regardless of the network state. Consequently, when the volume of conventional statistics declines noticeably, the value of routing overhead rises, but this is not a response of the protocol to the possibility of attack. In this rare circumstance, reactive AODV performs better.

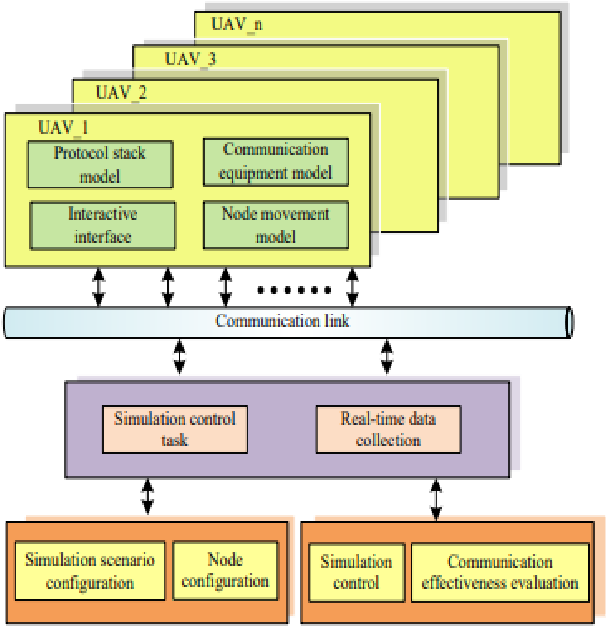

Fig. 8 : The structure of the UAV communication network simulation system.

DSR is a reactive source routing system that is intended for ad hoc networks with up to 200 mobile nodes. DSR, unlike other unicast routing protocols, does not maintain a routing database because it makes use of the source routing option in data packets. Instead, it takes use of Route Cache, which maintains an extensive list of IP addresses for each node in the path to the target. To put it another way, route discovery is unnecessary if a route to the sink is cached; but, if a route to the sink does not exist in the cache, route discovery must be performed by broadcasting a route request message. the source receives a response to the route request.

DSR and DSDV form the foundation of the AODV routing technology. It makes advantage of the DSR-like route finding process as well as the episodic beaconing and order enumeration of DSDV. DSR and AODV do differ significantly in two key ways, though. The key distinction between AODV and DSR is that whereas AODV just sends packets with the destination address, DSR sends packets with full routing information. Considering this, AODV could have lower routing overheads than DSR. The route answers in AODV only contain the sequence number and the destination IP address, but in DSR, they include the addresses of every node along the route. Being flexible to extremely dynamic networks is a benefit of AODV. When constructing a route, a node can face significant delays, and a broken link might force the identification of a new route. As the network grows, these additional delays and bandwidth use lead to increased network congestion.

The results of the publications cannot be directly compared in this part as the test settings and protocol aspects differ. Instead, the results of the routing protocols DSDV, DSR, and AODV are summarized and compared. The protocol behavior between the papers may be checked to determine if it is consistent. All investigations employ uniformly dispersed Endless Bit Rate (CBR) bases and bowls with random waypoints serving as the mobility model. There is a chance that CBR sources will not produce findings that apply to the actual world. Using this knowledge, the routing protocols are contrasted based on the system of measurement of amount, inexpression, and direction-finding upstairs. The quantity of minutes communicated among foundations and destinations per element of while, or the relation of communicated packages, is known as throughput, sometimes known as packet delivery fraction. The Fig. 9 gives the node model of UAV.

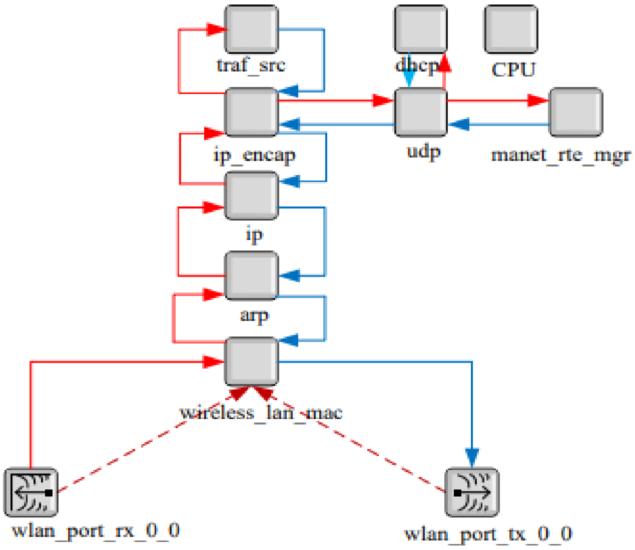

Fig. 9 : The node model of UAV.

An excessive number of CBR packets contributes to the delay. When traffic congestion becomes an issue, the postponement at little flexibility is larger than at intermediate movement since increasing mobility and traffic loads often increase the delay. The cause of this is congestion caused by several flows being routed via one network area. The average delay for DSR is the largest; under low loads, it has a shorter delay, but at high loads, AODV performs better. The increased number of nodes is, however, causing the DSDV's performance to degrade. Due to the mobility of nodes, both the load and frequency of routing table exchanges also rise.

The entire quantity of packets used for routing that are sent over the network is known as routing overhead. In line with rising mobility, the routing overhead rises. Due to the many route answers, it receives in response to a single route request, AODV has a larger routing overhead than DSR. The setup affects the DSDV routing overhead. As continuous route updates must be provided yet are constrained by a per node transmission period, it is both constant and independent of mobility. It first has a serial number that allows for the separation of the old from the new routing data. To save this serial number, a information turf is available in the topology control

(TC) group. The advantage of this is that it makes it possible for routing information to be updated and for TC packets to be transmitted randomly. As a result of the ongoing network interaction between the TC packets with this serial number, each node establishes one-hop and two-hop neighbor node information and maintains the topology of the entire wireless ad hoc network so that each node has a single hop or multi-hop path to the destination node. Packets are routed through this path during communication to reduce the end-to-end communication delay. The next technology is multipoint relay (MPR) . In contrast to the link state routing method, which chooses all of the one-hop neighbors as relay nodes, the OLSR protocol only selects the multipoint relay nodes that can build a symmetric link with all of the two-hop neighbor nodes. As the node only needs to send the link state data linked to the multipoint relay node in this way, the amount of TC packets sent over the network will be drastically reduced. When a one-hop neighbor node receives a broadcast packet, like the link status mechanism, it does not re-forward it. Decide whether it is the node's MPR node instead. It can forward the broadcast packet if the node is an MPR node. Using the technique results in a decrease in the length of the control packets, which also lowers the quantity of connections needed to transfer control messages. The update to IEEE 802.11s, here, we define a new category of mesh management for action management frames. The action field's value dictates what kind of management message will be sent. As an IEEE 802.11 information element, the actual message is displayed.

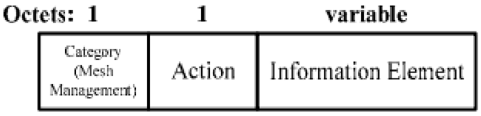

Fig. 10 : IEEE 802.11s mesh management action frame format

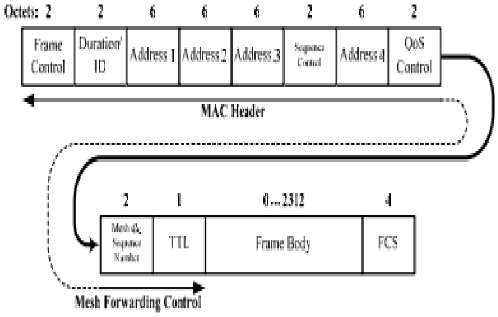

Fig. 11 : IEEE 802.11s mesh data frame format

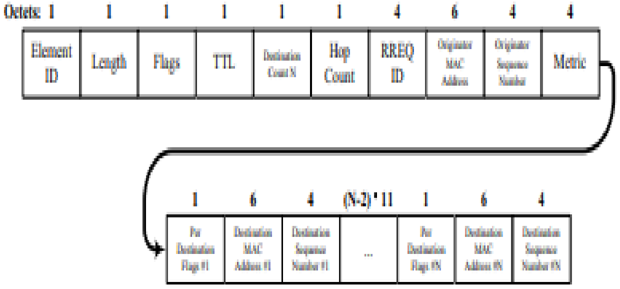

Fig. 12 : Structure of HWMP route request (RREQ) information element

The Figs. 10, 11 & 12 gives the IEEE 802.11s mesh management action frame format, IEEE 802.11s mesh data frame format & the structure of HWMP route request (RREQ) information elements. The main advantage of reactive routing is that it only determines a path when one is necessary to transmit data between two mesh nodes. There is a delay for the initial packet or packets because the computation of the path to the desired destination and the discovery of the connections with their characteristics do not start until after the first data packet has already arrived at the routing module of the foundation protuberance. Yet, if there is no traffic in the mesh network or if the road traffic decoration is not changing, this on-demand generation of the paths always uses the most recent link status data, such as from radio aware link measurements, and it reduces the routing overhead. The route-finding mechanism used by the Hybrid Wireless Mesh Protocols is well-known from AODV and DSR.

A route request message is broadcast by a foundation mesh point that needs a way to go to a last stop mesh point in order to complete its mission. Each mesh point processes and transmits the route request message, which establishes reversible pathways to the route discovery's initiator. If there are any intermediate mesh points on the way to the destination, they will also send a unicast route reply message as their answer. This is how the path leads to the destination is constructed. In order to comply with an IEEE 802 .11s path selection protocol's requirements, which include using layer 2 MAC addresses and radio-aware connection metrics, the route-finding technique has also been updated. The mechanisms of the HWMP reactive routing are more fully explained in the following sentences.

If there is already a path to the source mesh point S, the mesh point determines if it must be updated. The path to S is changed if the new path metric in the RREQ is superior to the path metric in the associated routing table entry and the sequence number of the RREQ is equal to or higher than the sequence number of the current routing table entry for the source mesh point S. The existing path to S is modified regardless of the value of the new path metric if the sequence number of the RREQ is higher than the sequence number of the linked routing table item by at least a specified threshold value. Additionally, if a more recent RREQ—one with a greater. The Fig. 13 give the configurability of HWMPs.

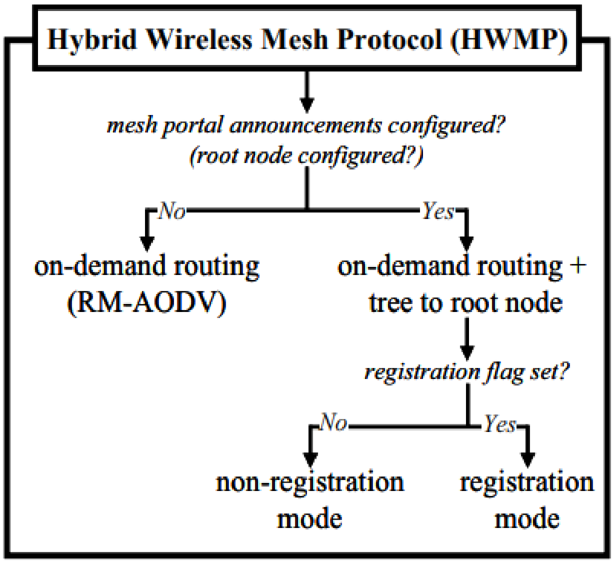

Fig. 13 : Configurability of HWMP

With a single RREQ message, HWMP enables simultaneous path discovery to numerous destinations. The destination count parameter indicates how many destination mesh points need to be found. The turfs per journey's end decorations, journey's end discourse, and terminus arrangement quantity are contained in the destination counts sequences of the RREQ. It is necessary to divide the RREQ control flags into two groups as a result. The matching per destination flags fields is set independently for each destination and contain the control flags that may differ in value for various destinations in the RREQ. As both the way demand and the course account travel the whole path and gather the most recent metric data, it guarantees that the found path metric is accurate. The flags field is set with control flags that are the same for all destinations in the RREQ. The broadcast (UB = 1) setting is the default for the unicast/broadcast flag (UB) . It has been presented for the HWMP proactive extensions. Instead of using the hop total steering measured, HWMP employs an arbitrary link metric, often a radio-aware one like the default airtime link metric discussed in section 6 . The quantity of relations in the trail is shown by the hop count field in the RREQ message, but it is not used to make a routing choice. Initial values for both the hop count and the metric are 0. The range of the RREQ is specified in terms of hops via the time to live field (TTL). Prior to generating a new route request, the source mesh point's RREQ ID counter is increased. The sequence number of the source mesh point, the originator, is increased by 1 if the route request will be utilized for route discovery.

In July 2004 , the IEEE 802.11 working group's research group for ESS mesh networking was renamed task groups "s" (TG's) . Its objective is to create a wireless mesh network standard that is versatile and extendable and is based on IEEE 802.11 . Radiocommunication multi-hop routing, which establishes the routes for radiocommunication promotion, is one of IEEE 802.11 s main features. IEEE 802.11s's scope and some specifications are defined in the PAR document. The IEEE 802.11 standard refers to mesh nodes as mesh points (MPs) . A station that supports both IEEE 802.11 and mesh is referred to as a mesh point. In accordance with the proposed 802.11s amendment, the term "mesh capabilities" refers to the ability to contribute in the net steering etiquette and to advancing information on behalf of other net facts. revealed in Figure 1 as the net grid.

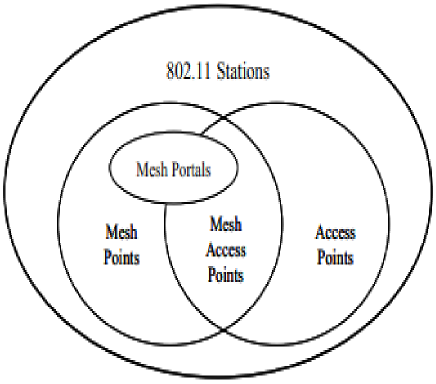

Fig. 14 : Relation amongst diverse IEEE 802.11 (mesh) nodes.

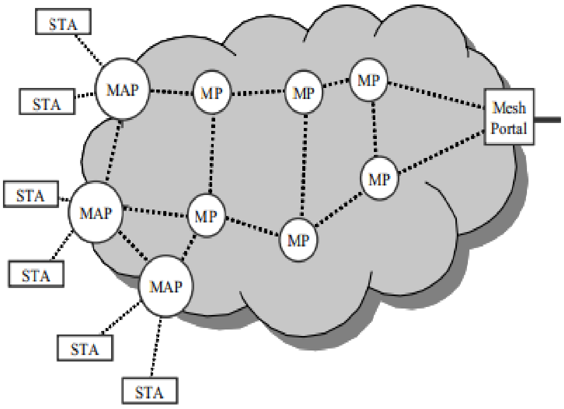

Fig. 15 : Example of an IEEE 802.11s WLAN net system

The Figs. 14 & 15 give the relation amongst diverse IEEE 802.11 (mesh) nodes and also an example of an IEEE 802.11s WLAN net system. A newfangled web information border format is defined by the IEEE 802.11s modification (Figure 3). When sending data within a WLAN mesh network, this MAC frame format is utilized. This format adds a mesh-specific control field to the already existing data frame format. The two flags to and from DS, as well as the type and subtype for the mesh data frame, are included in the frame control field together with additional control information. The two flags are set to 1 to indicate that the data frame is in the mesh network because it is part of the wireless distribution system. The four address fields include 48-bit MAC addresses, which are long. It is specified by the receiver address, or address 1, which mesh point must receive the wireless signal. The transmitter address, or 2, identifies the mesh point that sent this wireless data frame. Address 3v, which serves as the data frame's destination, indicates the final (layer 2) location of the data frame. This data frame's source is identified by address 4, which is the source address. The 3-byte-long mesh forwarding control field has two fields. The 16-bit long mesh end-to-end sequence number enables the broadcast flooding control and the transmission of ordered mesh data frames. Frames are uniquely identifiable by a source mesh e2e sequence number for a particular source mesh point. Throughout the forwarding of mesh data frames, the source mesh point establishes and maintains the mesh end-to-end sequence number. The 8-bit long time to live field (TTL) is used to time out mesh data frames that may have inadvertently become stuck in an endless forwarding loop. Sending commands for the path selection protocol requires the usage of management frames of type actions.

The hop count measure is more stable than a radio-aware routing metric. It is therefore advisable to gather and utilize the link metrics' most recent data. The respond and forward flag (RF) were implemented in order to eventually obtain the most recent route metric data. If the intermediate mesh points produced an RREP, the RF flag affects how the RREQ is sent. If the RF flag is set (RF = 1), the intermediary mesh point will forward (broadcast) the updated RREQ. In this situation, setting the terminus only flag to one (DO = 1) will prevent subsequent RREPs from the succeeding intermediate mesh points on the path to the intended destination. According to the established behavior of AODV, DO=0 , RF=0 should be used. After being unicast on the reverse path to the original mesh point S, the RREP message is sent from whatever mesh point created it. For each journey's end in the terminus count last stop in the RREQ message with multiple desired destinations, the decisions, and actions for the creation of RREPs must be taken. End point Di is deleted from the list of desired destinations in the RREQ if an RREP has been prepared for it and the RREQ does not need to be delivered to it in the event of an intermediate mesh point ($RF_i = 0$). The revised RREQ will be broadcasted together with the requests for any remaining destinations if there are any destinations in this list after all destinations have been processed. The RREQ will not be transmitted further if there is no destination remaining on the list of desired destinations.

Simulation Results

Simulations are performed & the results are observed. The Fig. 16 gives the average throughput for different routing protocols. (a) The number of nodes is 20 , the UAV speed is 10m/s (b) The number of nodes is 20, the UAV speed is 20m/s. (c) The number of nodes is 40, the UAV speed is 10m/s. (d) The number of nodes is 40, the UAV speed is 20m/s.

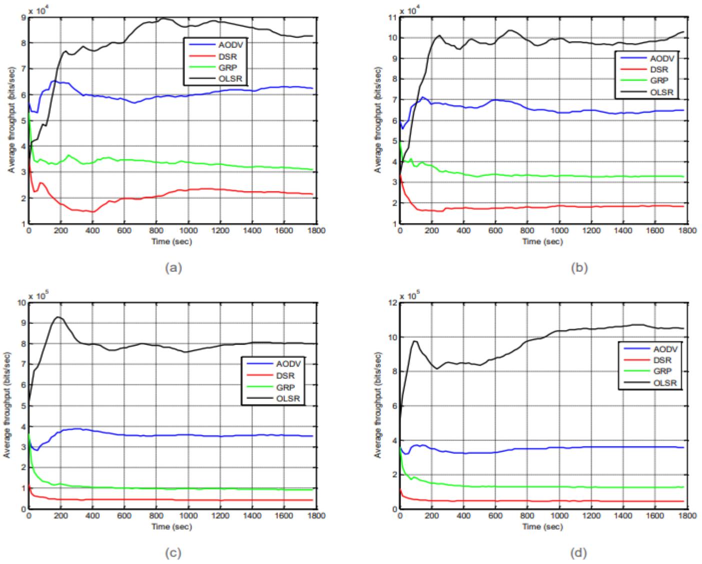

Fig. 16 : Average throughput for different routing protocols. (a) The number of nodes is 20 , the UAV speed is 10m/s (b) The number of nodes is 20, the UAV speed is 20m/s. (c) The number of nodes is 40, the UAV speed is 10m/s. (d) The number of nodes is 40, the UAV speed is 20m/s.

A dispersed, energy-efficient, region-based routing protocol called ER-RPL has been presented in this study. By utilizing network area information, ER-RPL combines proactive and reactive routing protocols. Generic traffic patterns may be supported by ER-RPL, which can also maximize efficiency and dependability. The adaptability and efficiency of ER-RPL have been confirmed via theoretical and experimental study. The choice made by ER-RPL is almost perfect. In terms of dependability and excellent energy saving, Internet of Things Journal 14 routes are quite effective. A significant decrease in routing overhead may be achieved with ER-RPL, and it is resistant to wireless channel conditions, according to thorough simulation data. The emphasis of this research is static networks, but we want to expand on this in subsequent work to include mobile networks. RPL is an anticipatory protocol that is designed for sensor-to-root (MP2P) message, where it offers minimum latency (if no loop occurs). RPL does, however, come with several drawbacks. First off, the protocol is not effective for root-to-sensor (P2MP) communication and is inappropriate for sensor-to-sensor (P2P) transmission since it was built with the implicit assumption that MP2P was the prevalent traffic pattern. In fact, the regulator signals (DAOs) for P2MP and P2P traffic appear to be a "afterthought" because the RPL description does not specify their emission schedule. Second, RPL places a unique need on the network's root node, making it a probable solitary fact of disappointment, a circulation bottleneck, and a universal route stretch for P2P traffic. Finally, when packets are routed via RPL, there is a significant probability of fragmentation and loops. Finally, RPL is inappropriate for networks with unidirectional links since it lacks link bi-directionality check procedures.

For ad hoc mobile networks, we describe many routing strategies in this article. We also categorize these schemes based on the routing technique (i.e., table-driven and on-demand). We have contrasted these two groups of 54 IEEE Personal Communications April 1999 routing technologies, showing their similarities and contrasts. Lastly, we have explored potential uses and difficulties posed by ad hoc mobile wireless networks. Each protocol has obvious benefits and drawbacks and is suitable for circumstances, even if it is unclear which algorithm or family of algorithms is the best in all instances. Although there are still many obstacles to overcome, the area of ad hoc mobile networks is expanding and changing quickly. It is expected that during the next few years, these networks will be widely used. The Figs. 17 & 18 gives the Packet Delivery Fraction-2.

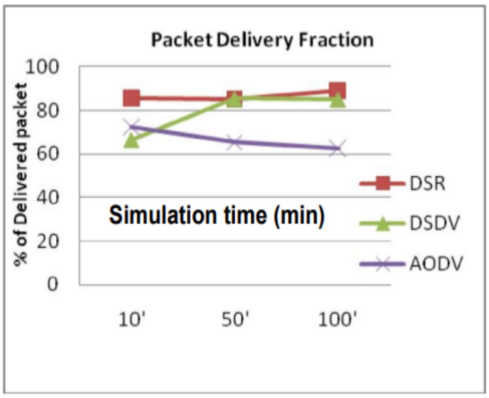

Fig. 17 : Packet Delivery Fraction-1

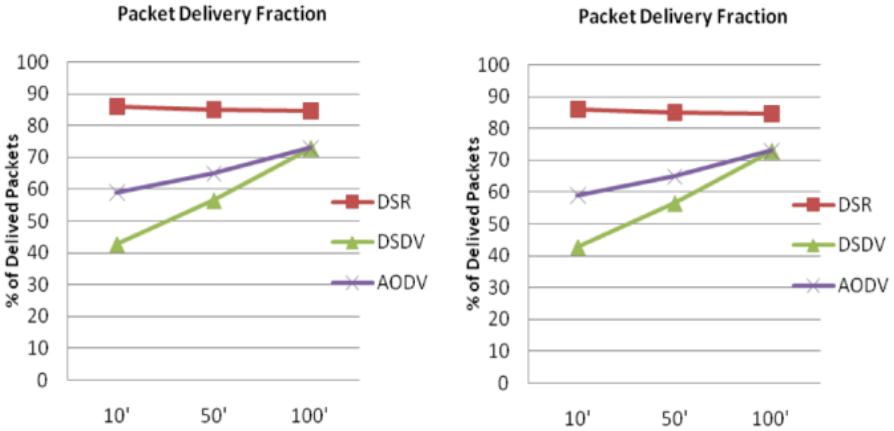

Fig. 18 : Packet Delivery Fraction-2

Comparision of different technologies

No.	Technology	Advantage	Disadvantage
1.	EDAL	High level security, quick response	Heavy Maintenance
2.	Wireless Sensor Network (WSN)	It is scalable, it is flexible	It cannot be used for high speed
3.	DSR	DSR allows multiple routes	does not automatically repair a broken link
4.	6LoWPAN	scalable and self-healing	less secure than ZigBee
5.	OLSR	implementation is more user friendly	bandwidth usage low for the maintaining of the routes
6.	Data Aggregation	Low quality data that is aggregated	lots of data aggregation and management solutions
7.	Geographic Routing	Easy-comparison of data items	retrieving geographic data is time-consuming
8.	IPv6 Routing protocol	Efficient Routing, Increased Capacity	System Issues, Device Upgrade

9.	IP/MPLS	Scalability, Efficiency	Security, Maintenance
10.	Load balancing	**Static IP Addresses Zonal Isolation**	**No SSL offloading**
11.	EDAL	High level security, quick response	Heavy Maintenance
12.	Wireless Sensor Network (WSN)	It is scalable, it is flexible	It cannot be used for high speeds
13.	DSR	DSR allows multiple routes	does not automatically repair a broken link
14.	6LoWPAN	scalable and self-healing	less secure than ZigBee
15.	OLSR	implementation is more user-friendly	bandwidth usage low for the maintaining of the routes
16.	Data Aggregation	Low quality data that is aggregated	lots of data aggregation and management solutions
17.	Geographic Routings	Easy comparison of data items	Retrieving geographic data is time-consuming
18.	IPv6 Routing protocol	Efficient Routing, Increased Capacity	System Issues, Device Upgrade
19.	IP/MPLS	Scalability, Efficiency	Security, Maintenance
20.	Load balancing	**Static IP Addresses, Zonal Isolation**	**No SSL offloading**

Conclusive Remarks

The routing protocol to deploy in a system that is crucial to operations has been determined after a comprehensive examination and judgement of the chosen routing protocols. Almost all recorded statistics showed that EIGRP regularly beat the other three procedures. Just the folder headwaiter packages to the ECC switch were measured, and in that case the other three protocols consistently beat EIGRP. EIGRP outscored the other routing protocols by a large margin, even though database access and traffic are an essential component of a public safety network. The speed of convergence is a crucial component of every network. In a network for public safety, when seconds count, this is extremely important. The decision here was EIGRP without a doubt. Although it would be logical to think that no new networks would be developed using FDDI because it is an obsolete technology, many public safety groups lack the funding and technological know-how that a private company could have. Despite this, EIGRP remains the ideal protocol to employ because it experienced the least amount of latency. The best routing protocol to adopt in a public safety network, according to an examination of the performance of RIP, OSPF, IGRP, and EIGRP, is EIGRP. The performance of the network if FDDI connections are replaced with a newer technology will be investigated and analyzed in the future.

This study offers a thorough analysis of IoT protocol options. The IETF, IEEE, ITU, and other organizations have created and standardized several of those protocols, and many more are constantly being developed. Due to the enormous quantity, the conversation was short. Referrals have thus been given for more information. This document aims to provide developers and service providers with information on the choices for various IoT protocol layers and how to select them. We alienated the study into four sections based on networking layers: information joining, system direction-finding, system encapsulation, and session layers. At each tier, we highlighted a few draughts and provided most of the standards that had been completed. We also addressed some of the current security standards and work done at various levels of standardization, as well as reviewing IoT management protocols briefly. We concluded by talking about several issues that still plague IoT devices and that scientists are working to resolve.

The extensible framework for routing with RA-OLSR as an optional standardized routing protocol, the ability to integrate optimized and vendor-specific routing protocols, and the configurable default routing protocol HWMP all contribute to IEEE 802.11s' broad applicability to a variety of wireless network usage scenarios. The information being provided is based on the initial draught of IEEE802.11s, which will change before it is officially accepted. The fundamental ideas behind the routing system, HWMP, and RA-OLSR, however, are well-established and solid. Even though it is quite possible that certain elements may alter, this merits a publishing like this. The work group "s" is actively examining and enhancing the draught standard. In response to suggestions from a preliminary internal evaluation, contributions have been made public. Later this year, during the first letter ballot, a lot of comments and adjustments are anticipated.

In conclusion, the examination of routing protocols within Low-Power and Lossy Networks (LLNs) has yielded crucial insights into their effectiveness and performance in practical scenarios. The study revealed notable variations in protocol performance, emphasizing the influence of factors such as network size, density, and topology. Energy efficiency emerged as a critical concern, emphasizing the need for protocols that balance data delivery with minimal energy consumption. Scalability challenges were identified, particularly in large-scale LLNs, prompting the call for protocols capable of accommodating network expansion. Robust fault tolerance mechanisms were underscored for maintaining reliability in LLN applications. Security considerations and the importance of standardization and interoperability were also highlighted. Ultimately, the conclusions drawn from this analysis provide a foundation for future research, guiding the development of resilient, energy-efficient, and scalable routing solutions tailored to the unique challenges of LLNs, contributing to the advancement of efficient and reliable communication in this evolving field.

References

1. Z. Jose, V.V. Sobral Joel, J.P.C. Rodrigues Ricardo, A.L. Raelo, Jalal Al-Mutadi & Valery Korotaev, ”Routing protocols for low power & low power and lossy networks in internet of things applications”, 9 May 2029.
2. Karim Rostamzadeh, Hasen Nicanfar, Narjes Torabi, Sathish Gopalakrishnan, Victor C.M. Leung, “A Context aware trust based information dissemination framework for vehicular networks”, IEEE Internet of Things Transactions, Vol. 2, No. 2, Apr. 2015.
3. Z. Safdar, S. Farid, M. Pasha, K. Safdar, “A security model for the IoT based systems”, Technical Journal, Univ. of Engg. & Tech. (UET), Taxila, Pakistan, Vol. 22, No. 4, ISSN : 1813-1786, 2017.
4. Shubhalika Dihulia, Tanveer Farooqui, “A survey on IoT security Challenges”, Int. Journal of Comp. Appliances, ISSN : 0975-8887, Vol. 169, No. 4, Jul. 2017.
5. Vandana Sharma, Ravi Tiwari, “Security on IoT & its smart appliances”, Int. Jour. of Science, Engg. & Tech. Research (IJSETR), Vol. 5, Issue 2, Feb. 2016.
6. Sachin Updadhya, “Ongoing challenges & research opportunities”, Int. Jour. of Engg. Technologies & Management Research, Vol. 5, No. 2, Special Edition, pp. 216-222, DOI : 10.6281/Zefnodo.1195065
7. Wei Zhou, Yuging Zhang, Peng Liu, “Effect of IoT new features on security & privacy”, The college of Info. Sciences & Tech., The Pennsylvania State Uni., PA, 16802, USA.
8. Saeed Banaeian Far Azadeh Imani Rad, “Security analysis of Big Data on IoT”, IEEE Transactions in Industrial Electronics, Vol. 12, Issue 3, ISSN : 1232-1242, 2016.
9. Mirza Abdur Razzaq, Mohammed Ali Qureshi, Sajid Habib Gill, Saleem Ullah, “Security issues in IoT”, IJASCA, Int. Jour. of Adv. Comp. Sci. & Appliances, Vol. 8, No. 6, 2017.
10. Hui Suo, Jiafu Wan, Caifeng Zou, Jianqi Liu, “A review on security in IoT”, 2012 IEEE Int. Conf. of Comp. Sci. & Engg., 2012.
11. Xiaopeng Tan, Zhen Zuo, Shaojing Su, Xiaojun, Guo, Xiaoyong Sun, Deng Jiang. “Performance Analysis of Routing Protocols for UAV Communication Networks”, IEEE Access, 2020.
12. Accettura, Nicola, Maria Rita Palattella, Mischa Dohler, Luigi Alfredo Grieco, and Gennaro Boggia, “Standardized power efficient & internet-enabled communication stack for capillary M2M networks”, 2012 IEEE Wireless Communications and Networking Conference Workshops (WCNCW), 2012.
13. Zheng Min Wang, Wei Li, Hui Liang Dong, “Analysis of Energy Consumption and Topology of Routing Protocol for Low-Power and Lossy Networks”, Journal of Physics: Conference Series, 2018.
14. Md Anam Mahmud, Ahmed Abdelgawad, Kumar Yelamarthi, “Improved RPL for IoT Applications”, 2018 IEEE 61st International Midwest Symposium on Circuits and Systems (MWSCAS), 2018
15. Kumar, Neeraj, and Mayank Dave, “A Beacon Information Independent VANET Routing Algorithm with Low Broadcast Overhead”, International Journal of Computer Network and Information Security, 2015.\
16. Michael Bahr, “Proposed routing for IEEE 802.11s WLAN mesh networks”, Proceedings of the 2nd annual international workshop on Wireless internet – WICON’06, 2006
17. Ivascu, G.I., “QoS routing with traffic distribution in mobile ad hoc networks”, Computer Communications, 20090212
18. Xiongwei Ren, Jianqi Zhang, “Review of the Cross-Layer Design in Wireless Ad Hoc and Sensor Networks”, 2010 International Conference on Computational Intelligence and Software Engineering, 2010.
19. Watteyne, T., & Pister, K. S. (2011). "Stress testing the Internet of Things: The mctest framework." In 2011 8th IEEE International Conference on Mobile Ad-Hoc and Sensor Systems (MASS) (pp. 529-534).
20. Dohler, M., Watteyne, T., Winter, T., & Barthel, D. (2012). "Towards a reliable internet of things: A survey." Journal of Sensor and Actuator Networks, 1(2), 101-139.

21. Gnawali, O., Fonseca, R., Jamieson, K., Moss, D., & Levis, P. (2009). "Collection tree protocol." In Proceedings of the 7th ACM Conference on Embedded Networked Sensor Systems (SenSys) (pp. 1-14).
22. Duquennoy, S., Al Nahas, B., Landsiedel, O., & Johansson, P. (2013). "Let the tree bloom: Scalable opportunistic routing with ORPL." In Proceedings of the 11th ACM Conference on Embedded Networked Sensor Systems (SenSys) (pp. 1-14).
23. Hui, J. W., Culler, D., Chakrabarti, S., & Levis, P. (2008). "The dynamic behavior of a data dissemination protocol for network programming at scale." In Proceedings of the 6th ACM Conference on Embedded Network Sensor Systems (SenSys) (pp. 81-94).
24. Thubert, P., & Watteyne, T. (2016). "Industrial Routing Requirements in Low-Power and Lossy Networks." RFC 7774, Internet Engineering Task Force (IETF).
25. Brandt, A., Buron, J., & Toutain, L. (2014). "Survey of Routing in Low Power and Lossy Networks: Background and Overview." RFC 6553, Internet Engineering Task Force (IETF).