International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 11 Issue: 04 | Apr 2024 www.irjet.net p-ISSN: 2395-0072

To evaluate the proposed routing protocol across several networks circumstances

Thrisha V.S[1], Dr.Anitha T.N[2]

[1]*Assistant Professor, Dept. of CS&E, Sir. M Visvesvaraya Institute of Technology, Bangalore*
[2]*Professor & Head, Dept. of CS&E, Sir. M Visvesvaraya Institute of Technology, Bangalore*

Abstract - *This Internet of Things (IoT) has become one of the greatest noteworthy areas of computing because to the quick development of technology and internet-connected gadgets. IoT ecosystem-targeting standards, technologies, and platforms are being created quickly. For a variety of uses, including healthcare, home automation, disaster recovery, and industry automation, IoTv makes it possible for things to communicate and plan activities. It is anticipated that it will eventually cover even more applications. This article examines several standards developed by the IEEE , IETF , and ITU that support technologies allowing the explosive rise of IoT . To fulfil the needs of the IoT , these standards encompass protocols for the communications , routing , network , and session layers. The issue also includes management and security standards, providing details on the research being done to address these difficulties in addition to the current IoT challenges. We propose simulation-based research to put a number on how important a cross-layer design is for better-quality QoS sustenance in radiocommunication ad hoc systems. Using the J-Simv simulator, we contrast the layered architecture utilizing the AODV routing protocol with the CROSS-LAYER Engine design using QoS-PARv as a routing protocol. We make use of J-Sim since cross-layer implementations are suited for it. In addition to the recommended routing protocol, QoS-PAR , and the LYMP protocol, we used it to create the entire CROSS LAYERv Engine architecture. The movement of nodes in mobile ad hoc networks frequently changes the network structure, making routing in MANETs a challenging problem. The efficient routing algorithms could considerably benefit mobile ad hoc networks in terms of performance and reliability. Such networks have been the subject of several routing protocol proposals thus far. There have been some studies published in the literature evaluating the performance of suggested routing protocols under CBR traffic with various network conditions, but little attention has been paid to evaluating their performance when applied to traffic generators other than CBR , such as FTP , TELNET , etc . The complexity of traffic in actual applications is not reflected by CBR traffic , and the traffic scenarios described here are more like the network loads experienced by MANETs in the real world. This article examines the performance of the three routing protocols AODV , DSR , and WRP for FTP , TELNET , and CBR traffic in terms of packet delivery ratio, throughput, average end-to-end delay, and routing message overhead. Many network circumstances are considered, including the effects of modifying the halt length and the quantity of source destinations. For the consolidation and centralization of the public safety network's main services, it is essential to assess which routing protocol provides the best performance and throughput in a mission-critical setting. The following routing protocols are evaluated: Routing Information Protocol (RIP), Open Shortest Path First (OSPF), Interior Gateway Routing Protocol (IGRP), and Enhanced Interior Gateway Routing Protocol (EGIRP). Convergence , throughput , and queuing delay are also evaluated. The network is simulated using Riverbed Modeler Academic Edition 17.5v . According to a study of the results, which procedure should be utilized.*

Key Words: IoT, GSM, RPL, RFID.

1. INTRODUCTION

This document is template. We ask that authors follow A similar approach has been used for radio ad hoc and instrument systems due to the Internet's widespread popularity, which is largely due to its layered design. Unfortunately, a rigid layered structure is not adaptable enough to deal with the changing situations, which will obstruct performance improvements. Due to the unpredictability and unreliability of the underlying radiocommunication intermediate, cross-layer design research in radiocommunication instrument grids and ad hoc networks has recently attracted a lot of attention. Many studies have been undertaken on various elements of the cross-layer design. Finding a method for each layer's abstraction and an appropriate coupling mechanism is essential for successful cross-layer optimization. Cross-layer design may be broadly split into layer trigger scheme , joint optimization scheme , and complete cross-layer design depending on how many layers (single , multiple , or whole) are engaged in optimizations. In both wired and wireless networks, layer triggers—predefined signals that alert to situations like data transmission problems between protocols—are often utilized. Samples contain the Obvious Cramming Announcement method, which alerts the receiver whenever network congestion happens, and the L2 trigger, which is inserted among the link and Disposable etiquette coating to effectively notice variations in the condition of radiocommunication systems.

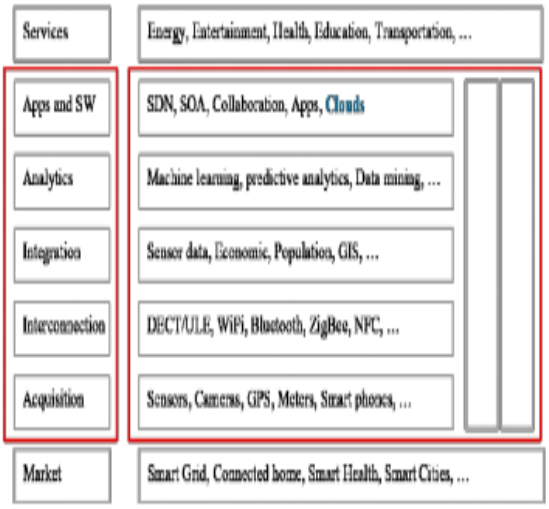


Fig 1: The IoT Ecosystem

The coat gun trigger technique offers optimization and benefits by taking a perpendicular crosscut across the sheets while retaining the current protocol stack in the foreground. These triggers may be set off on a regular basis by network events or an adaptive control system. Although if more than two tiers of the protocol stack may be included in such a trigger mechanism, only a particular layer component oversees other parts at upper- or lower-layer layers harvest relevant parameters and provide them to the defined layer, which is where the optimization process is taking place. For instance, a control loop based on cross-layer information shared between the medium access and network layers is proposed, the physical layer transmission mode used to predict link stability and link lifetime is monitored, route rearrangement protocols are enabled to act quickly and prevent route breaks and packet loss, TCP is the most popular transport and the foundation for various other protocols in both wired and wireless networks . The prolonged hidden-/exposed-terminal issue, however, leads to poor end-to-end connection, which negatively impacts TCP's performance in multi hop IEEE 802.11 networks. In order to solve these issues, cross-layer interaction of TCP and ad hoc routing protocols , there are some suggested options, like the TCP fractional window increment scheme and the route-failure notification using bulk-loss trigger policy. Without altering the core TCP window or the wireless MAC process, these protocols allow for the separation of congestion from other network events.

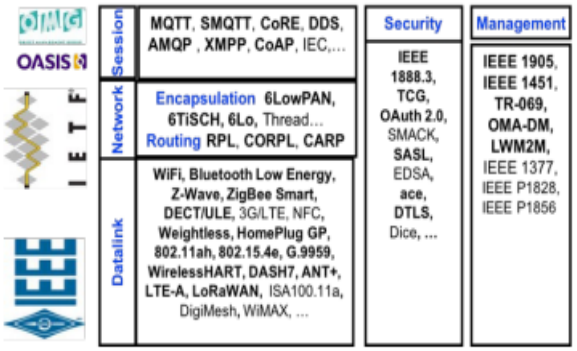


Fig 2: Protocols of IoT

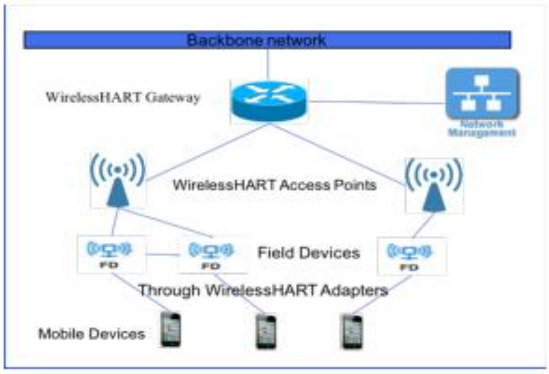


Fig 3: wirelessHART Architecture

During the last several years, wireless mesh networks have drawn more attention. Wireless mesh networks (WMNs) is being installed at an increasing rate. There are several prosperous new businesses, or "mesh firms." Their brands are well-known now that they are selling mesh equipment and providing wireless mesh solutions to customers even though they have been in business for a long. Wireless mesh networks are receiving more attention and publications as a result of the growing number of press reports and publications on them. The numerous new WMN standards organizations and the significant interest in them are another sign of the increasing notice in radiocommunication web grids. Network mesh WLANs are standardized by IEEE 802.11s . Network schmoozing for radiocommunication private part networks is a focus of IEEE 802.15.5 . The term wireless multi-hop relaying is defined by IEEE 802.16j . Over traditional wireless LANs , wireless mesh networks offer more performance , flexibility , and dependability . Wireless communication between nodes through several radiocommunication journeys on a mesh net diagram is the primary feature of wireless mesh networking.

Effective routing protocols offer routes done the radiocommunication web and respond to active vicissitudes in the network topology so that mesh nodes may interact with one another even if they are not straight in radio

variety of one another. The packets will be sent to the destination via intermediate nodes on the route. The foundation of mobile ad hoc networks (MANETs) is the same: effective routing techniques for wireless meshed network graphs and wireless multi-hop communication. MANET -specific routing techniques are often used in wireless mesh networks. The same fundamental ideas underlie both radio net systems and moveable ad hoc systems, however they place differing emphasis on certain factors. With an emphasis on end-user strategies, movement, and ad hoc capabilities , MANETs emerged from an academic setting. As opposed to this, WMNs have a commercial background and concentrate mostly on still strategies, frequently organization strategies, dependability, network capacity , and, of course, practical implementation. Between WMNs and MANETs , however, there is no clear distinction. Articles or publications that use both terms together do so to show how closely related they are. Nowadays, public wifi access is the most well-known use for wireless mesh networks. WLAN access points are dispersed throughout cities, as well as on college and corporate campuses, and the wireless mesh network offers a customizable backhaul for them. In you may find a study on radio network systems. Included in is a summary of routing in WMNs . This article describes the suggested routing for the future IEEE 802.11s WLAN mesh networking standard. The present draught standard D0.01 from March 2006 serves as the basis for the document.

2 RELATED WORKS

[1] A Review of Current Routing Protocols Ad Hoc Mobile Wireless Networks , the author of this paper describes more than a few direction-finding strategies for ad hoc moveable systems. 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 routing methods, showing their similarities and differences. 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 some circumstances, even if it is unclear which algorithm or family of algorithms is the best in all circumstances. Although there are still many obstacles to overcome, the area of ad hoc mobile networks is expanding and changing quickly. It is expected that over the next few years, these networks will be used extensively.

[2] Av Survey of Protocols and Standards for Internet of Things , in this research, it is shown how the Internet of Things (IoT) has become one of the greatest important areas of computing thanks to the fast development of technology and internet-connected gadgets. A lot of ground is being made in the development of standards, technologies, and platforms for the IoT ecosystem. Health care, homebased mechanization, tragedy retrieval, and business mechanization are just a few of the frequent areas where the Internet of Things (IoT) enables things to communicate and coordinate actions In the future, further applications are anticipated to be added. This article examines several standards developed by the IEEE , IETF , and ITU that support the technologies allowing the explosive expansion of the IoT . To address the needs of the Internet of Things, these standards encompass protocols for the infrastructures, direction-finding, net, and meeting layers. The topic includes the current IoT challenges as well as management and safety values, providing information on the research being done to address these difficulties.

[3] Proposed Routing for IEEE 802.11s WLAN Mesh Networks , based on the current draught standard D0.01 from March 2006 , this research gives a description of the planned direction-finding for IEEE 802.11s WLAN web systems. An extensible framework for routing is defined by IEEE 802.11s , along with a new mesh data frame type. It describes HWMP , the standard routing protocol. AODV is the foundation of HWMP , which also contains a customizable postponement for practical direction-finding near so-called web doorways. For layer 2 routing, it makes use of MAC addresses, and while determining pathways, it employs a radio-aware routing metric. There is also information on the RA-OLSR optional routing protocol. Note that, at the time of writing, work is still being done to standardize WLAN Mesh Networking in IEEE 802.11s . The suggested routing protocols' specifics are likely to evolve, even though their fundamental ideas appear to be fairly set. It also offers a comprehensive analysis of the planned routing for the future IEEE 802.11s WLAN mesh network standard. IEEE 802.11s' comprehensive pertinency to a variety of radiocommunication network usage scenarios is a result of the configurable evasion steering procedure HWMP , the extensible outline for steering with RA-OLSR as an elective consistent steering etiquette, and the aptitude to participate improved and vendor-specific steering etiquettes. 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 are, nonetheless, widely accepted and very robust. 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. The IEEE 802.11s standard is anticipated to receive its final certification in 2008 .

[4] 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.

[5] 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 ad hoc 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 QoSPAR 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.

[6] 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 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.

[7] 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 ad hoc 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.

[8] 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 andv 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 DSDV . 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.

[9] 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 analysing 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.

[10] 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.

3.METHODOLOGY

In July 2004 , the IEEE 802.11 working group's research group for ESS mesh networking was renamed task group "s " (TGs) . 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.

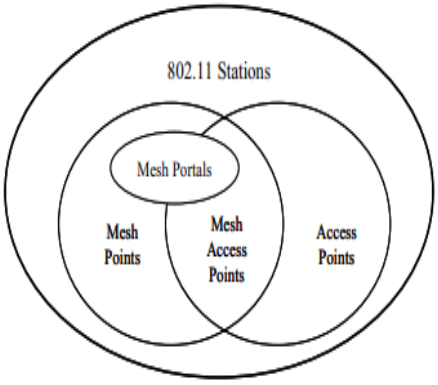


Fig: Relation among diverse

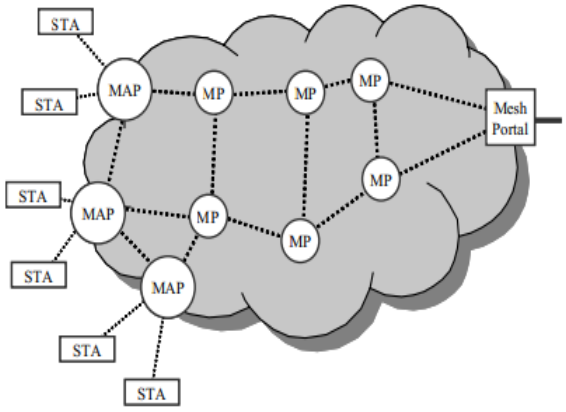


Fig: Example of an IEEE 802.11 sIEEE 802.11 (mesh) nodes.

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 action. The update to IEEE 802 .11s defines 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.

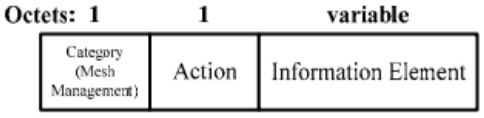
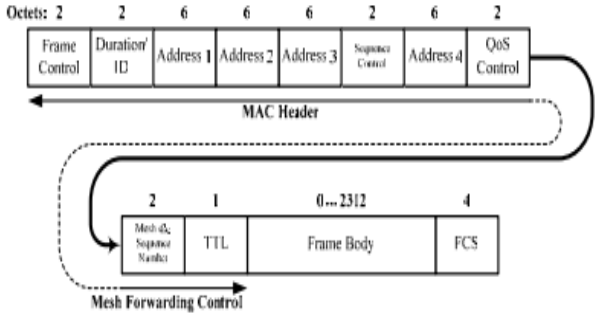


Fig: IEEE 802.11s mesh management action frame format



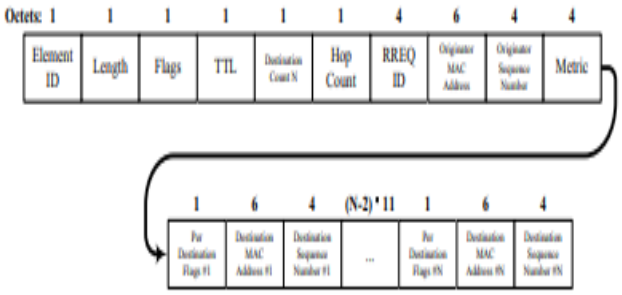


Fig: IEEE 802.11s mesh data frame format
Fig: Structure of HWMP route request (RREQ) information element

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 Protocol 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.

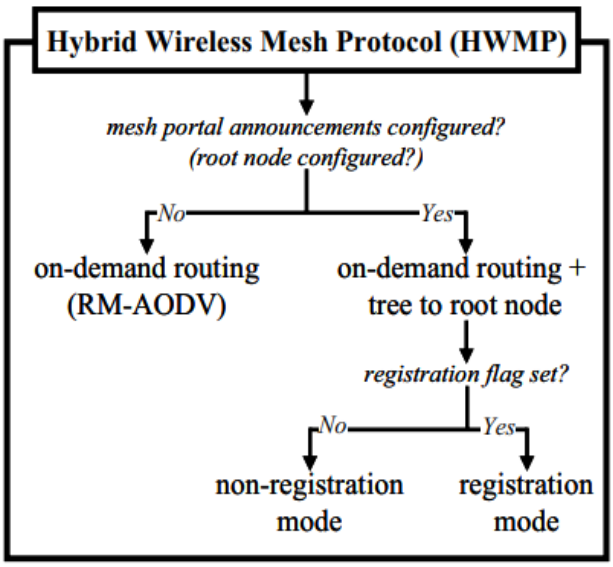


Fig: Configurability of HWMP

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 are 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.

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 point 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 (RFi=0). The revised RREQ will be broadcast vtogether 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.

Table -1: COMPARISON OF DIFFERENT TECHNOLOGIES

SL 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**

4. CONCLUSIONS

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.

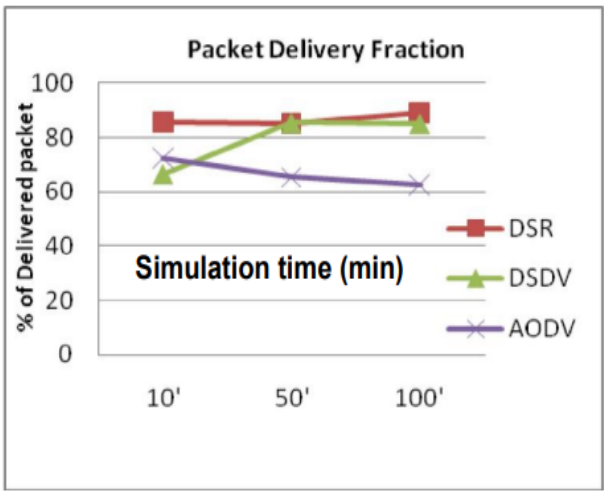


Fig 4: Packet Delivery Fraction1

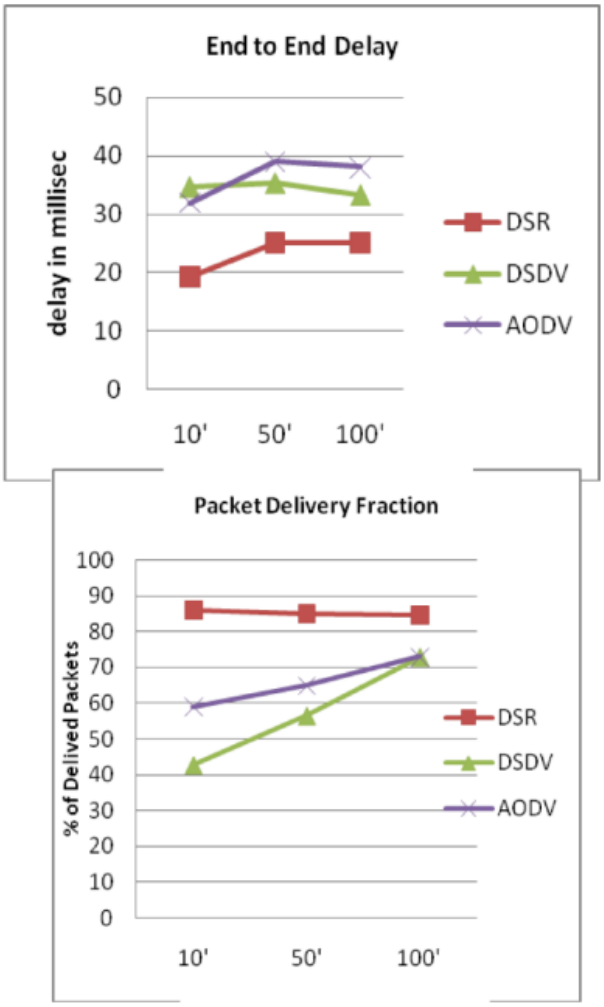


Fig 5: Packet Delivery Fraction2

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.

REFERENCES

[1]Z José V. V. Sobral Joel J. P. C. Rodrigues Ricardo A. L. Rabêlo , Jalal Al-Muhtadi and Valery Korotaev , " Routing Protocols for Low Power and Lossy Networks in Internet of Things Applications " in Received : 23 March 2019 ; Accepted : 5 May 2019 ; Published : 9 May 2019

[2] Karim Rostamzadeh , Student Member , IEEE , Hasen Nicanfar , Student Member , IEEE , Narjes Torabi , Student Member , IEEE , Sathish Gopalakrishnan , Member , IEEE, and Victor C. M. Leung , Fellow , IEEE, "A Context-Aware Trust-Based Information Dissemination Framework for Vehicular Networks " in IEEE INTERNET OF THINGS JOURNAL , VOL. 2 , NO. 2, APRIL 2015

[3] [1]Z. Safdar , S. Farid , M. Pasha , K. Safdar , " A Security Model for IoT based Systems " in Technical Journal , University of Engineering and Technology (UET) Taxila , Pakistan vol.22 No. 4-2017 ISSN:1813-1786 (print) 2313-7770(online)

[4]Shubhalika Dihulia, Tanveer Farooqui , "A Survey on IoT Security Challenges " in International Journal of Computer Appliances (0975-8887) volume 169 – No.4, July 2017

[5]Vandana Sharma , Ravi Tiwari " Security on IoT and its Smart Appliances " in International Journal of Science , Engineering and Technology Research (IJSETR), volume 5, Issue 2, February 2016

[6]Sachin Upadhyay "Ongoing Challenges and Research Opportunities " in International Journal of Engineering Technologies and Management Research , 5(2:SE) ,216-222 . DOL :10.6281/Zenodo .1195065

[7]Wei Zhou , Yuqing Zhang , Peng Liu "Effect of IoT new features on security and privacy " in The College of Information Sciences and Tcehnology , The Pennsylvania State University , PA 16802,USA

[8]Saeed Banaeian Far , Azadeh Imani Rad "Security analysis of Big Data on IoT " in IEEE transactions in Industrial informatics 12.3(2016) : 1232-1242

[9]Mirza Abdur Razzaq , Muhammad Ali Qureshi , Sajid Habib Gill , Saleem Ullah "Security Issues in IoT " in (IJASCA) International Journal of Advanced Computer Science and Appliances , volume 8, No.6,2017

[10]Hui Suo , Jiafu Wan, Caifeng Zou, Jianqi Liu "A Review on Security in IoT" in 2012 Intenational Conference on

BIOGRAPHIES

Dr. T.N. Anitha,
Professor & Head,
Dept of CSE, Sir. MVIT
Bangalore

Ms. Thrisha V.S,
Assistant Professor
Dept of CSE, Sir. MVIT
Bangalore