INJ INTERNATIONAL NEUROUROLOGY JOURNAL

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

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 idea behind the Internet of Things (IoT) is causing a important expansion of the Internet's volume to gather, examine, and disseminate data that may be used to create information or data. Direct connection between IoT devices of different sorts is presented to create specific environments that are intelligent and self-aware. Many minor devices and low control plans are part of one class of technologies, such as Low Power Lossy Networks (LLNs), which serve as the foundation for the Internet of Things. The Routing Protocol for LLNs (RPL), the central component of the Internet of Things (IoT),To our knowledge, there has not been much done in the way of RPL experimentation and assessment. There are a few simulation tools available that allow for the evaluation of RPL in a realistic deployment environment. In order to grasp RPL's role in the Internet of Things, this study focuses on understanding its architecture and protocol stack. Regarding performance parameters like packet delivery ratio, latency, signaling overhead, and energy usage, simulations in the Contiki OS Cooja simulator are used to test RPL's performance in a hypothetical Smart Health setting. The simulation findings demonstrate that the RPL has demonstrated several appropriate properties that may make it beneficial for wider scale deployments. A collection of mobile nodes connected by wireless links to create a temporary network without a predetermined topology, centralized access point, or infrastructure is known as a mobile Adhoc network. Each node in such a network has the ability to serve as both a router and a host simultaneously, and it is free to quit or join the network as necessary. This study has already covered several routing protocols, but it will now compare two reactive protocols—DSR and AODV—as well as one proactive protocol, DSDV. When using position-based routing, a thorough analysis of the network's performance, including throughput, overhead, delay, and pause time, is performed. Variable simulation times are used to investigate performance variations as mobility and location inaccuracy have an impact on node performance. With the help of the NS-2vvsimulator, the simulations are run. The findings highlight how critical it is to carefully consider and execute routing methods in an ad hoc setting. The Low power and Lossy Networks for the Smart Grid require a robust routing protocol. The procedures are castoff to forward data, which contains facts gathering, information distribution, and other activities. In order to understand their advantages and disadvantages, this study compares RPL and LOAD, the two primary routing protocols for Low-powerv and Lossy Networks. Based on an examination of the specification and experimental data, observations are made on the routing overhead, traffic patterns, resource requirements, fragmentation, and other aspects of the protocol. The performance of various traffic patterns, such as sensor-to-sensor, sensor-to-root, and root-to-sensor bidirectional traffic, is further investigated using simulations. The readers might pick the most suitable protocol for their intended applications by assessing various protocols in order to have a better grasp of their applicability. 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.

INJ INTERNATIONAL NEUROUROLOGY JOURNAL

The network is simulated using Riverbed Modeler Academic Edition 17.5vv. According to a study of the results, which procedure should be utilized.

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

Introduction

Public safety organizations have the chance to operate at a greater degree of interoperability thanks to increased information availability and sharing. As a result, the public will receive services that are of a higher caliber. The computer network, which enables communication and the exchange of crucial information among the major players, is at the heart of every operation involving public safety and information sharing. Public safety organizations frequently operate on a limited budget and must make due with outdated tools and technology in order to deliver services.

If the network is set properly, it is feasible to make a public safety network work with older equipment that can handle heavy demands. Choosing the right routing protocol choice is crucial to this arrangement. For the network to continue operating at a reasonable level in the case of a breakdown, routing procedures must be in place to guarantee that crucial packets are delivered accurately and effectively. Distance vector techniques for routing, such RIP and IGRP, demand that the router communicate its whole routing bench with its near nationals at the predetermined inform intermission. Small private networks are best suited for RIP.

\With the help of the link state protocol OSPF, routers may exchange details around their individual straight linked neighbors, and updates are then forwarded to other routers. Only data concerning network changes is transmitted when network convergence has been attained. Large private networks are best suited for OSPF. As it combines the best elements of both link state and distance vector protocols, EIGRP is categorized as a hybrid routing protocol. Medium to big private networks are where it operates best. This study aims to model a tall request, mission-critical public safety network connecting two distinct towns. The planned network's main information hub is the Emergency Communications Center. Links between nodes in this system are made using FDDI. The Fig. 1 gives the schematic diagram of AODV path finding process.

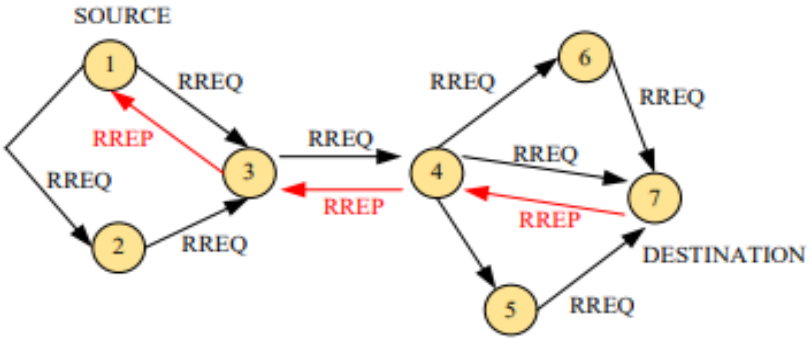

Fig. 1 : Schematic diagram of AODV path finding process

In RPL, a DAG (i.e., a gradient) is created by defining how link costs and node attributes/status must be coupled in order to compute route costs given a set of sinks. Available energy resources, workload, throughput, latency, dependability, and other factors can be included in link prices and node information. In other words, RPL uses an objective function, which may be specified in a variety of ways to allow for extremely high flexibility about the operating environment, to minimize the expenses to reach any sink (from any sensor). Moreover, RPL closely respects to the IPv6 architecture: gradient is started up and maintained via signaling messages sent as options of IPv6 Router Advertisements (RA). RPL isolates packet processing and forwarding from the routing optimization goal in order to be applicable in a variety of LLN application areas. For effective P2P communications, our suggested ER-RPL uses the region data. The region that a node is in is crucial information for static networks like M2M systems and wireless sensor networks (WSNs). This area functionality is utilized by several LLN apps. For instance, using automated switch schemes, a switch facility may be delivered to all the equipment in a level, area, or room of a structure. The location of the sensor that captured the data may not matter in event-triggered applications because all nearby devices can record the occurrence. You may effectively find the routing pathways by using the region information. The Fig. 2 gives the routing protocol classifications.

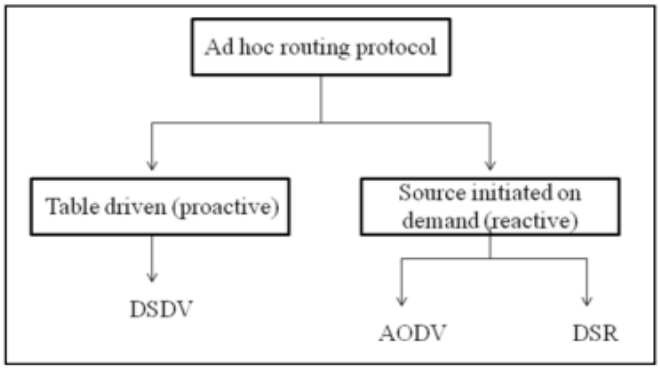

Fig. 2 : Routing Protocol Classification

Instead, then using nodes' IP addresses, geographic routing forwards data packets in a greedy fashion using the locations of nodes (either actual or virtual coordinates). In order to relay its data packets, a node choose the neighboring node that is the most nearby to the destination. Each node, or set of partial nodes, determines the position or coordinate using either a priori information or a self-configuring localization strategy. Geography routing has the benefits of low routing upstairs and scalability support, but it does not consider the lossy nature of wireless networks when picking the next hop. Geographic routing thus frequently struggles to provide consistent data delivery support for LLNs over the lossy wireless medium. Some geographic routing methods additionally require nodes to constantly exchange the one-hop or even two-hop neighbor database in order to maintain the coordinates. The Fig. 3 gives the flow chart of DSR route discovery.

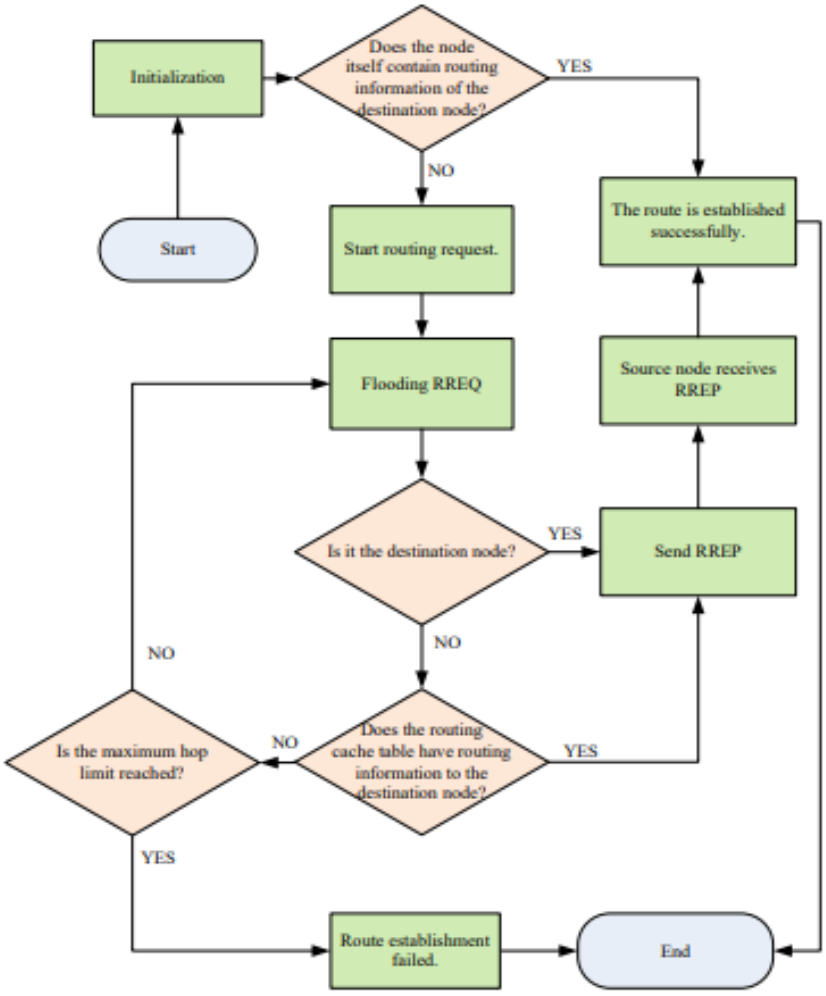

Fig. 3 : The flow chart of DSR route discovery.

A network with limited resources finds it to be quite expensive in terms of energy usage. Think of the node density in each zone as being equal. The Self-Regioning method allows a node to construct four regions per RN after identifying the nearest one. And about a rectangle-shaped area defines each zone Similar to this, three neighboring RNs may be utilized to produce six regions per RN if the region shape is like a hexagon. The Self-regioning method may create octagonal regions if four more neighbor RNs are employed. The Self-regioning method allows each RN to have two areas if additional nearby RNs are included after determining the nearest RN. In this manner, when NRN/s is present in the network, there are 2N regions. There are more regions since the Self regioning process involves more RNs. Just a small sample of areas are investigated by ER-RPL for choosing the best P2P route. A lesser subdivision of protuberances often participates in way detection when the network is split into multiple areas, each of which is smaller in size. More RNs can be employed in the Self-regioning method in order to reduce control overhead in this manner. The Fig. 4 gives the flow chart of DSR route maintenance.

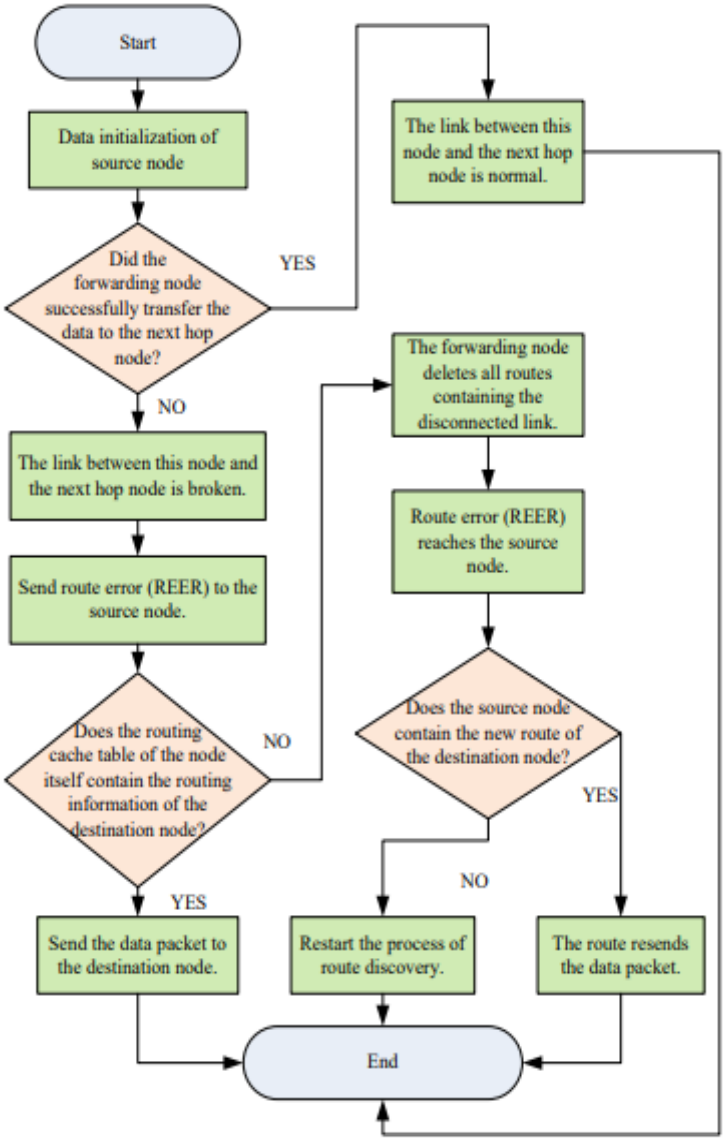

Fig. 4 : The flow chart of DSR route maintenance.

During the region-based route discovery process, each node in the IRCM regions selects the best possible route to the destination node. Nodes nearby the source or destination node transfer their routing information (source routing or hop-by-hop routing) to the destination node in the interim. The destination node may then support all downwards routes from the temporary root (the destination node in this routing pair) to every node in the source node's region and the destination node's area. To make communication between the regions of the source node

ISSN:2093-4777 | E-ISSN:2093-6931
DOI: 10.5123/inj.2023.4.in144
Vol. 27 Iss. 4 (2023)

and the destination node easier, the DODAG root, the destination node in this P2P pair, acts as an intermediary. In addition, each node keeps an R2R table, where each row represents a node. 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. The Fig. 5 gives the IoT Ecosystem's block-diagram.

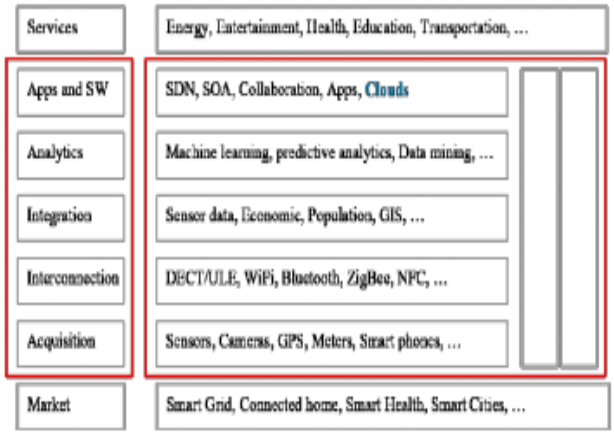

Fig. 5 : The IoT Ecosystem

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 Adhoc 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. The Fig. 6 gives the various protocols of the IoT system, whereas the Fig. 7 gives the Wireless HART Architectures.

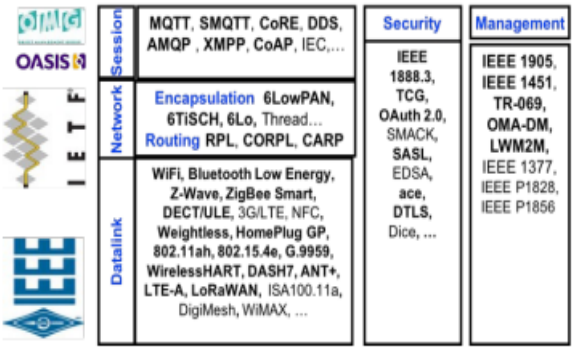

Fig. 6 : Protocols of IoT

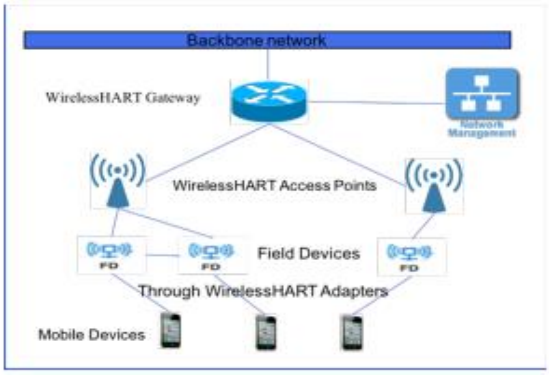

Fig. 7 : Wireless HART Architecture

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 Adhoc systems, however they place differing emphasis on certain factors. With an emphasis on end-user strategies, movement, and Adhoc 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 D0.01from March 2006 serves as the basis for the document.

Related Works – Literature Review

A number of researchers had worked on the proposed topic that is taken up for research in this paper. To mention a few of them are given below.

[1] Performance Analysis of Routing Protocols for UAV Communication Networks, the design of the routing protocol, according to the study's author, is one of the main problems that UAV communication networks must deal with. In low-altitude situations, information transmission by UAVs is challenging. A significant scientific challenge is creating a routing system that can deliver reliable and efficient packet transit from node to node. In this work, four conventional routing protocols—Adhoc on Demand Distance Vector (AODV), Dynamic Source Routing (DSR), Optimized Link State Routing (OLSR), and Geographic Routing Protocol—are put to the test in a more accurate simulation environment based on OPNET 14.5 (GRP). Data loss, throughput, network latency, and other performance parameters are compared and analyzed. The experimental findings suggest that several

routing strategies can be adapted to different UAV communication network configurations. The quantitative data could provide helpful direction for choosing the best routing protocol in various situations.

[2] Internet of Things and RPL Routing Protocol : A Study and Evaluation, this study presents the hypothesis that the Internet of Things (IoT) is significantly increasing the Internet's capacity to collect, analyze, and share data that may be utilized to produce knowledge or information. Direct connectivity between IoT devices of various types is suggested as a technique to develop settings that are intelligent and self-aware. One class of technologies, such as Low Power Lossy Networks (LLNs), which form the basis of the Internet of Things, includes a lot of tiny sensors and low-power gadgets. The Internet Engineering Task Force's ROLL working group developed the Routing Protocol for LLNs (RPL), which forms the basis of the Internet of Things (IoT) protocol stack used for communication between these low-power devices. According to our understanding, there has not been any experimentation or assessment of RPL. There are a few simulation programs that enable RPL assessment for a realistic deployment situation. The purpose of this article is to better understand RPL's architecture and protocol stack, and consequently the role it plays in the Internet of Things. About performance parameters like packet delivery ratio, latency, signaling overhead, and energy usage, simulations in the Contiki OS Cooja simulator are used to test RPL's performance in a hypothetical Smart Health setting. According to the simulation findings, the RPL has demonstrated a few desirable traits that might make it beneficial for deployments at a broader scale.

[3] Performance Evaluation and Comparison of Routing Protocols in MANETS, This research offers With no permanent topology, centralized access point, or other infrastructure, a mobile Adhoc network is made up of several mobile nodes connected by wireless links. Each node in such a network could function both as a router and host at the same time, and it is free to leave or join the network as needed. This study has already covered several routing protocols, but it will now compare two reactive protocols—DSR and AODV—as well as one proactive protocol, DSDV. When position-based routing is employed, a thorough analysis of the network's performance is done, including throughput, overhead, latency, and pause time. Variable simulation times are used to investigate performance variance as mobility and location inaccuracy have an impact on node performance. Using the NS-2 simulator, the simulations are run. The results show how crucial it is to carefully assess and apply routing protocols in an ad hoc setting.

[4] Analysis of Routing Protocol Performance in Wireless Mesh Networks, The aim of this study is to evaluate and compare proactive and reactive routing methods that have been adapted for usage with wireless mesh networks from ad hoc networks. The research of protocol performance is based on the findings of multistage simulations for both TCP and UDP traffics, as well as for both a healthy, functional network and a network with an injected selfish node. We recommend following steps in such cases. This paper's goal is to assess and contrast proactive and reactive routing systems that have been modified for use with wireless mesh networks from ad hoc networks. Based on the outcomes of multistage simulations for both TCP and UDP traffic, as well as for both a healthy, functioning network and a network with an injected selfish node, the study of protocol performance is based on protocol performance. In some situations, we advise employing specialized methods.

[5] Performance Analysis of the RPL Routing Protocol, we give an in this study and The IPv6 Routing Protocol for Low power and Lossy Networks, or RPL protocol, has recently been suggested by the IETF Routing Over Low-power and Lossy Networks working group. It was made to meet the common needs of wireless sensor networks. This research offers a performance analysis of RPL based on simulations due to its applicability in the scientific and industrial communities. Our findings unequivocally demonstrate that RPL can ensure a very quick network setup, enabling the creation of sophisticated monitoring applications even under challenging circumstances. The RPL signaling, however, must be improved in order to reduce protocol overhead, as we discovered.

[6] Evaluation of Routing Protocol for Low Power and Lossy Networks : Loading and RPL, The Routing protocol, according to this study's author, is a key component of Low power and Lossy Networks for Smart Grid. The protocols are employed in data forwarding, which also involves information sharing and data gathering. For lossy and low-power networks, two well-known routing methods are compared in this paper. must be able to distinguish between RPL's and loading's benefits and drawbacks. There are observations made about the resource demand, traffic patterns, fragmentation, routing overhead, etc. study of the specification and experimental data led to a modification of the protocol. Simulators are also being launched in order to study how different traffic patterns, such as sensor-to-sensor, sensor-to-root, and sensor-to-sensor bidirectional traffic, work. By assessing such protocols, readers might have a better knowledge of the protocols' applicability and

ISSN:2093-4777 | E-ISSN:2093-6931
DOI: 10.5123/inj.2023.4.in144
Vol. 27 Iss. 4 (2023)

select the best protocol for their intended uses. With Loading, the simulation took 25 hours, while for RPL, it took 270 seconds. Because DAO messages are sent periodically2 in the simulation (5 seconds per packet), the time needed to conduct the simulation would have been several days, and trace files would have grown to hundreds of Gigabytes per simulation. For this reason, 24 hours for RPL was not chosen. Although the simulation runs considerably more quickly and can simulate a 24-hour period, it is like loading in that no control traffic is transmitted when no data traffic is supplied. Even though the simulation times varied, the results (0.1 seconds per data request for RPL, and 30

[7] An Energy-efficient Region-based RPL Routing Protocol for Low-Power and Lossy Networks, Introducing the in this study are the general architecture of the Internet of Things includes routing, which is crucial. For Low-Power and Lossy Networks interoperability, the IETF has standardized the RPL routing protocol (LLNs). Applications for LLNs range widely, and include industrial control, healthcare, building automation, and others. Applications running on LLNs require dependable and energy-efficient routing support. A key prerequisite for many LLNs applications is point-to-point (P2P) connectivity. To find a trustworthy P2P route, conventional routing techniques, on the other hand, typically propagate around the whole network, consuming a significant amount of energy. Reliability and energy efficiency might be difficult to accomplish at the same time, especially for LLNs. In this research, we provide ER-RPL, a novel energy-efficient region-based routing protocol that provides reliable energy-efficient data transfer. The key to energy savings in the suggested strategy is that only a portion of nodes are required to complete the operation. The suggested approach only needs a fraction of nodes to complete the task, as opposed to current routing protocols that demand all nodes for route discovery. ER-RPL beats two other benchmark protocols, RPL and P2P-RPL, in terms of performance, according to our extensive simulation experiments and theoretical study.

[8] Analysis of Routing Protocols in an Emergency Communications Center, in this paper, we focus on the. Routing protocols are used in every network to decide the optimum routes to and from different hosts for packet routing. This paper presents a hypothetical logical network for a cooperative Emergency Communications Center (ECC) connecting two municipalities. To consolidate and centralized the vital activities of the public safety network, it is necessary to evaluate which routing protocol offers the best speed and throughput in a mission-critical setting. Convergence, throughput, and queuing time are tested for four different routing protocols: Which procedure to be used may be determined by analyzing the findings. A computer network is essential to any activity involving public safety and information sharing since it allows for communication and the exchange of crucial data among the major players. Public safety organizations frequently operate on a limited budget and must make due with outdated tools and technology in order to deliver services. If the network is set properly, it is feasible to make a public safety network work with older equipment that can handle heavy demands. Choosing the right routing protocol choice is crucial to this arrangement. For the network to continue operating at a reasonable level in the case of a breakdown, routing procedures must be in place to guarantee that crucial packets are delivered accurately and effectively. Distance vector routing techniques like RIP and IGRP demand that the router share its whole routing table with its immediate neighbor's every time an update occurs. The best RIP candidates are tiny private networks. Routers can share information about their own directly linked neighbors with other routers using a link state protocol known as OSPF. Only information regarding network changes is handed on once network convergence has been established. Large private networks are the ideal candidates for OSPF. Since it combines the best elements of link state and distance vector protocols, EIGRP is categorized as a hybrid routing protocol.

[9] Performance Evaluation of Routing Protocol for FANET Using NS2, In this study, we focus on a network called a Flying Ad-hoc Networks (FANETs), which is made up of a group of small, wirelessly connected unmanned aerial vehicles (UAVs) that cooperate together to score goals from the highest position. FANET's had gained popularity recently, both in the realm of technology and in research and development. When end-to-end data is sent from one UAV to another in FANETs, routing protocols are essential. Fast, scalable, self-configured networks may be provided via FANETs. There are several routing protocols in use today, and each one has its own problems. The major goal of this analysis is to compare the various routing protocols, including AODV, DSDV, DSR, and OLSR, based on metrics like throughput, end-to-end latency, and the number of nodes. Military uses for the autonomous flying vehicles include tracking adversaries and their movements as well as ongoing border surveillance activities. Applications in medicine for the transplanting of medications and even organs; applications in agriculture for the spare use of pesticides and insecticides; applications in forestry for the detection of fires; applications in agriculture for the spare surveillance of plants and fields; etc. Systems for unmanned aerial vehicles (UAVs) have the option of being autonomous or remote-controlled. Common names for UAVs include drones. Unmanned aerial vehicles (UAVs) are made to fly autonomously and be remotely operated by a person on the ground. UAVs are equipped with wireless transceivers for communication

with other UAVs or ground-based equipment, a microcontroller for processing input commands, the ability to be remotely controlled from outside, and other features. Via single or multichip communication, every node of a UAV is connected to a base station. A UAV network consists of a wireless system for data transmission, a GPS unit for location tracking, cameras for taking pictures and videos, different sensors for detecting desired parameter values, etc. Every day, more people are using UAVs.

[10] Performance Analysis of the Objective Functions in IPv6 Routing Protocol for LLN's used in IOT Applications, in this study, the Internet of Things network comprises of intelligent devices that are linked to one another and used in industries including industrial monitoring, healthcare, the military, automatic meter reading, and environment. A low power and lossy network (LLN) are what this network is because of the limited resources and the busy workplace. One important aspect affecting how well LLNs work is the design of the routing algorithm. The IETF ROLL working group has suggested the RPL (IPv6 Routing protocol for LLN's), which was created specifically for LLN's. By using a set of parameters and constraints defined inside the chosen objective function, this protocol aims to construct a destination-oriented DAG. The two standard OFs that are listed in this process (OF0) are MRHOF (Minimum rank with Hysteresis Objective Function) and 0 (Objective Function). The DODAG is produced as a result of the Objective Function selection made during network building, and this in turn affects important variables like Power Consumption, among others. The goal of this study is to evaluate RPL performance for light and medium density networks using the COOJA simulator running on the Contiki-2.7 OS. MRHOF outperforms OF0 for networks with up to 70 nodes, according to the simulation findings, in terms of energy consumption. Across 110 nodes, MRHOF and OF0's performance are observed to be equivalent.

[11] A Review of Current Routing Protocols Adhoc Mobile Wireless Networks, the author of this paper describes more than a few direction-finding strategies for Adhoc 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.

[12] A 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.

[13] Proposed Routing for IEEE 802.11s WLAN Mesh Networks, based on the current draughts 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.

Conclusions

The work that is being carried out in this paper is extended to the next part – II in the next paper.

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).